

DEFENDANTS' EXHIBIT 129:

DOJ 18-198 (D.O.J.), 2018 WL 920088

Department of Justice (D.O.J.)

Deputy Attorney General (DAG)

(NEWS RELEASE)

**GRAND JURY INDICTS THIRTEEN RUSSIAN INDIVIDUALS AND THREE RUSSIAN
COMPANIES FOR SCHEME TO INTERFERE IN THE UNITED STATES POLITICAL SYSTEM**

February 16, 2018

The Department of Justice announced that a grand jury in the District of Columbia today returned an indictment presented by the Special Counsel's Office. The indictment charges thirteen Russian nationals and three Russian companies for committing federal crimes while seeking to interfere in the United States political system, including the 2016 Presidential election. The defendants allegedly conducted what they called "information warfare against the United States," with the stated goal of "spread[ing] distrust towards the candidates and the political system in general."

"This indictment serves as a reminder that people are not always who they appear to be on the Internet," said Deputy Attorney General Rod J. Rosenstein. "The indictment alleges that the Russian conspirators want to promote discord in the United States and undermine public confidence in democracy. We must not allow them to succeed. The Department of Justice will continue to work cooperatively with other law enforcement and intelligence agencies, and with the Congress, to defend our nation against similar current and future schemes. I want to thank the federal agents and prosecutors working on this case for their exceptional service. Also, we received exceptional cooperation from private-sector companies like Facebook and Paypal."

According to the allegations in the indictment, twelve of the individual defendants worked at various times for Internet Research Agency LLC, a Russian company based in St. Petersburg, Russia. The other individual defendant, Yevgeniy Viktorovich Prigozhin, funded the conspiracy through companies known as Concord Management and Consulting LLC, Concord Catering, and many subsidiaries and affiliates. The conspiracy was part of a larger operation called "Project Lakhta." Project Lakhta included multiple components, some involving domestic audiences within the Russian Federation and others targeting foreign audiences in multiple countries.

Internet Research Agency allegedly operated through Russian shell companies. It employed hundreds of persons for its online operations, ranging from creators of fictitious personas to technical and administrative support, with an annual budget of millions of dollars. Internet Research Agency was a structured organization headed by a management group and arranged in departments, including graphics, search-engine optimization, information technology, and finance departments. In 2014, the agency established a "translator project" to focus on the U.S. population. In July 2016, more than 80 employees were assigned to the translator project.

Two of the defendants allegedly traveled to the United States in 2014 to collect intelligence for their American political influence operations.

To hide the Russian origin of their activities, the defendants allegedly purchased space on computer servers located within the United States in order to set up a virtual private network. The defendants allegedly used that infrastructure to establish hundreds of accounts on social media networks such as Facebook, Instagram, and Twitter, making it appear that the accounts were controlled by persons within the United States. They used stolen or fictitious American identities, fraudulent bank accounts, and false identification documents. The defendants posed as politically and socially active Americans, advocating for and against particular political candidates. They established social media pages and groups to communicate with unwitting Americans. They also purchased political advertisements on social media.

The Russians also recruited and paid real Americans to engage in political activities, promote political campaigns, and stage political rallies. The defendants and their co-conspirators pretended to be grassroots activists. According to the indictment, the Americans did not know that they were communicating with Russians.

After the election, the defendants allegedly staged rallies to support the President-elect while simultaneously staging rallies to protest his election. For example, the defendants organized one rally to support the President-elect and another rally to oppose him-both in New York, on the same day.

On September 13, 2017, soon after the news media reported that the Special Counsel's Office was investigating evidence that Russian operatives had used social media to interfere in the 2016 election, one defendant allegedly wrote, "We had a slight crisis here at work: the FBI busted our activity.... So, I got preoccupied with covering tracks together with my colleagues."

The indictment includes eight criminal counts. Count One alleges a criminal conspiracy to defraud the United States, by all of the defendants. The defendants allegedly conspired to defraud the United States by impairing the lawful functions of the Federal Election Commission, the U.S. Department of Justice, and the U.S. Department of State in administering federal requirements for disclosure of foreign involvement in certain domestic activities.

Count Two charges conspiracy to commit wire fraud and bank fraud by Internet Research Agency and two individual defendants.

Counts Three through Eight charge aggravated identity theft by Internet Research Agency and four individuals.

There is no allegation in the indictment that any American was a knowing participant in the alleged unlawful activity. There is no allegation in the indictment that the charged conduct altered the outcome of the 2016 election.

Everyone charged with a crime is presumed innocent unless proven guilty in court. At trial, prosecutors must introduce credible evidence that is sufficient to prove each defendant guilty beyond a reasonable doubt, to the unanimous satisfaction of a jury of twelve citizens.

The Special Counsel's investigation is ongoing. There will be no comments from the Special Counsel at this time.

DOJ 18-198 (D.O.J.), 2018 WL 920088

DEFENDANTS' EXHIBIT 130:

2021 WL 808994
Bloomberg Government
Copyright (c) 2021 Bloomberg Government

Testimony
March 2, 2021

House of Representatives
Financial Services

Committee Hearing FBI Oversight/Current Security Threats

CQ Abstract

Committee:

Senate Judiciary Committee

Subject:

FBI Oversight/Current Security Threats

Abstract:

Senate Judiciary Committee (Chairman Richard J. Durbin, D-Ill.) hearing on ‘Oversight of the Federal Bureau of Investigation: the January 6 Insurrection, Domestic Terrorism, and Other Threats.’

Scheduled Witnesses:

Christopher Wray, Director, Federal Bureau of Investigation

Sen. Charles E. Grassley, R-Iowa

COMMITTEE TESTIMONY

March 2, 2021

Christopher Wray, Director, Federal Bureau of Investigation, Washington, DC

Committee:

Senate Judiciary Committee

Subject:

FBI Oversight/Current Security Threats

Testimony:

Good morning, Chairman Durbin, Ranking Member Grassley, and Members of the Committee. I am honored to be here, representing the men and women of the FBI. Our people -- nearly 37,000 of them -- are the heart of the Bureau. I am proud of their service and their commitment to our mission. Every day, they tackle their jobs with perseverance, professionalism, and integrity - sometimes at the greatest of costs.

Just last month, two of our agents made the ultimate sacrifice in the line of duty. Special Agents Dan Alfin and Laura Schwanzenberger left home to carry out the mission they signed up for - to keep the American people safe. They were executing a federal court-ordered search warrant in a violent crimes against children investigation in Sunrise, Florida, when they were shot and killed. Three other agents were also wounded that day. We'll be forever grateful for their commitment and their dedication - for their last full measure of devotion to the people they served and defended. We will always honor their sacrifice.

Despite the many challenges our FBI workforce has faced, I am immensely proud of their dedication to protecting the American people and upholding the Constitution. Our country has faced unimaginable challenges this past year. Yet, through it all, whether it was coming to the aid of our partners during the Capitol siege and committing all of our resources to ensuring that those involved in that brutal assault on our Democracy are brought to justice, the proliferation of terroristic hate moving at the speed of social media, abhorrent hate crimes, COVID-19 related fraud and misinformation, the increasing threat of cyber intrusions and state-sponsored economic espionage, malign foreign influence and interference, the scourge of opioid trafficking and abuse, or human trafficking and crimes against children, the women and men of the FBI have unwaveringly stood at the ready and taken it upon themselves to tackle any and all challenges thrown their way.

The list of diverse threats we face underscores the complexity and breadth of the FBI's mission: to protect the American people and uphold the [Constitution of the United States](#). I am pleased to have received your invitation to appear today and am looking forward to engaging in a thorough, robust, and frank discussion regarding some of the most critical matters facing our organization and the Nation as a whole.

Capitol Violence

First and foremost, I want to assure you, your staff, and the American people that the FBI has deployed every single tool at our disposal and our full arsenal of investigative resources to aggressively pursue those involved in the heinous violence and criminal activity that occurred on January 6, 2021. We are working closely with our federal, state, and local law enforcement partners, as well as private sector partners, to identify those responsible for the violence and destruction of property at the U.S. Capitol building who showed blatant and appalling disregard for our institutions of government and the orderly administration of the democratic process.

Our agents, analysts, and professional staff have been working non-stop with federal prosecutors to gather and preserve evidence, share intelligence, and identify and bring charges against those who participated in the siege of the U.S. Capitol. As we have said consistently, we do not and will not tolerate violent extremists who use the guise of First Amendment-protected activity to wreak havoc and incite violence. Thus far, our investigators have identified hundreds of individuals involved in the siege of the Capitol Complex and already charged well over 300 of them. Many of those identifications are the result of the over 200,000 digital media tips we have received from the public. Members of the public who have any information related to the siege should continue to provide tips, information, and videos of illegal activity at www.tips.fbi.gov or by calling 1-800-CALL-FBI.

Overall, the FBI assesses that the January 6th siege of the Capitol Complex demonstrates a willingness by some to use violence against the government in furtherance of their political and social goals. This ideologically motivated violence underscores the symbolic nature of the National Capital Region and the willingness of Domestic Violent Extremists to travel to events in this area and violently engage law enforcement and their perceived adversaries. The American people should rest assured that we will continue to work to hold accountable those individuals who participated in the violent breach of the Capitol on January 6th, and any others who attempt to use violence and destruction to intimidate, coerce, or influence the American people or affect the conduct of our government.

Top Terrorism Threats

As has been stated multiple times in the past, preventing terrorist attacks, in all forms, remains the FBI's top priority. The nature of the threat posed by terrorism - both international terrorism ('IT') and domestic terrorism ('DT') - continues to evolve.

The most significant threat to our homeland is posed by lone actors who often radicalize online and seek out soft targets to attack with easily accessible weapons. We see these individualized threats manifested within both Domestic Violent Extremists ('DVEs') and Homegrown Violent Extremists ('HVEs'). Although they have different ideologies, they both typically radicalize and mobilize to violence on their own and are both located primarily in the United States. Individuals who commit violent criminal acts in furtherance of ideological goals stemming from domestic influences - some of which include racial or ethnic bias, or strong anti-government or anti-authority sentiments - are described as DVEs, whereas HVEs are individuals inspired primarily by achieving global jihad, but not receiving individualized direction from Foreign Terrorist Organizations ('FTOs').

Domestic and Homegrown Violent Extremists are often motivated and inspired by a mix of socio-political, ideological, and personal grievances against their targets, and more recently have focused on accessible targets to include civilians, law enforcement and the military, symbols or members of the U.S. Government, houses of worship, retail locations, and mass public gatherings. Selecting these types of soft targets, in addition to the insular nature of their radicalization and mobilization to violence and limited discussions with others, challenges law enforcement to detect and disrupt the activities of lone actors before they occur.

The top threat we face from DVEs continues to be those we identify as Racially or Ethnically Motivated Violent Extremists ('RMVEs'), specifically those who advocate for the superiority of the white race, and who were the primary source of ideologically-motivated lethal incidents of violence in 2018 and 2019. It is important to note that we have recently seen an increase in lethal DVE attacks perpetrated by Anti-Government or Anti-Authority Violent Extremists, specifically Militia Violent Extremists and Anarchist Violent Extremists. Anti-Government or Anti-Authority Violent Extremists were responsible for three of the four lethal DVE attacks in 2020. Also, in 2020, we saw the first lethal attack committed by an Anarchist Violent Extremist in over 20 years.

Consistent with our mission, the FBI does not investigate First Amendment-protected speech or association, peaceful protests, or political activity. The FBI holds sacred the rights of individuals to peacefully exercise their First Amendment freedoms. Non-violent protests are signs of a healthy democracy, not an ailing one. Regardless of their specific ideology, the FBI will aggressively pursue those who seek to hijack legitimate First Amendment -protected activity by engaging in violent criminal activity such as the breach, destruction of property, and violent assaults on law enforcement officers that we witnessed on January 6th and during lawful protests throughout the U.S. during the summer of 2020. In other words, we will actively pursue the opening of FBI investigations when an individual uses - or threatens the use of - force, violence, or coercion, in violation of federal law and in the furtherance of a political or social ideological goal.

The FBI assesses HVEs as the greatest, most immediate international threat to the Homeland. As I have described, HVEs are United States-based individuals, located in and radicalized primarily in the U.S., who are not receiving individualized direction from global jihad-inspired FTOs, but are inspired largely by the Islamic State of Iraq and ash-Sham ('ISIS') and al-Qa'ida to commit violence. An HVE's lack of a direct connection with an FTO, ability to rapidly mobilize without detection, and use of encrypted communications pose significant challenges to our ability to proactively identify and disrupt them.

The FBI remains concerned that Foreign Terrorist Organizations, such as ISIS and al-Qa'ida, intend to carry out or inspire large-scale attacks in the U.S. Despite their loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners - both here at home and overseas. To this day, ISIS continues to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. ISIS' successful use of social media and messaging apps to attract individuals seeking

a sense of belonging is of continued concern to us. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have at times specifically advocated for attacks against soldiers, law enforcement and other intelligence community personnel.

Al-Qa'ida maintains its desire for large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, in the near term, al-Qa'ida is more likely to continue to focus on building its international affiliates and supporting small-scale, readily achievable attacks in regions such as East and West Africa. Over the past year, propaganda from al-Qa'ida leaders sought to inspire individuals to conduct their own attacks in the United States and other Western nations.

Iran and its global proxies, including Iraqi Shia militant groups, continue to attack and plot against the United States and our allies throughout the Middle East in response to U.S. pressure. Iran's Islamic Revolutionary Guard Corps-Qods Force ('IRGC-QF') continues to provide support to militant resistance groups and terrorist organizations. Iran also continues to support Lebanese Hizballah and other terrorist groups. Lebanese Hizballah has sent operatives to build terrorist infrastructures worldwide. The arrests of individuals in the United States allegedly linked to Lebanese Hizballah's main overseas terrorist arm, and their intelligence collection and procurement efforts, demonstrate Lebanese Hizballah's interest in long-term contingency planning activities here in the Homeland. Lebanese Hizballah Secretary-General Hasan Nasrallah also has threatened retaliation for the death of IRGC-QF Commander Soleimani.

As an organization, we continually adapt and rely heavily on the strength of our federal, state, local, Tribal, territorial, and international partnerships to combat all terrorist threats to the United States and our interests. To that end, we use all available lawful investigative techniques and methods to combat these threats while continuing to collect, analyze, and share intelligence concerning the threat posed by violent extremists, in all their forms, motivated by any ideology, who desires to harm Americans and U.S. interests. We will continue to share information and encourage the sharing of information among our numerous partners via our Joint Terrorism Task Forces across the country, and our Legal Attache offices around the world.

Lawful Access

The problems caused by law enforcement agencies' inability to access electronic evidence continue to grow. Increasingly, commercial device manufacturers have employed encryption in such a manner that only the device users can access the content of the devices. This is commonly referred to as 'user-only-access' device encryption. Similarly, more and more communications service providers are designing their platforms and apps such that only the parties to the communication can access the content. This is generally known as 'end-to-end' encryption. The proliferation of end-to-end and user-only-access encryption is a serious issue that increasingly limits law enforcement's ability, even after obtaining a lawful warrant or court order, to access critical evidence and information needed to disrupt threats, protect the public, and bring perpetrators to justice.

The FBI remains a strong advocate for the wide and consistent use of responsibly-managed encryption - encryption that providers can decrypt and provide to law enforcement when served with a legal order. Protecting data and privacy in a digitally- connected world is a top priority for the FBI and the U.S. government, and we believe that promoting encryption is a vital part of that mission. But we have seen that the broad application of end-to-end and user-only-access encryption adds negligible security advantages. It does have a negative effect on law enforcement's ability to protect the public. What we mean when we talk about lawful access is putting providers who manage encrypted data in a position to decrypt it and provide it to us in response to legal process. We are not asking for, and do not want, any 'backdoor,' that is, for encryption to be weakened or compromised so that it can be defeated from the outside by law enforcement or anyone else. Unfortunately, too much of the debate over lawful access has revolved around discussions of this 'backdoor' straw man instead of what we really want and need.

We are deeply concerned with the threat end-to-end and user-only-access encryption pose to our ability to fulfill the FBI's duty of protecting the American people from every manner of federal crime, from cyber-attacks and violence against children to drug trafficking and organized crime. We believe Americans deserve security in every walk of life - in their data, their streets, their businesses, and their communities.

End-to-end and user-only-access encryption erode that security against every danger the FBI combats. For example, even with our substantial resources, accessing the content of known or suspected terrorists' data pursuant to court-authorized legal process is increasingly difficult. The often online nature of the terrorist radicalization process, along with the insular nature of most of today's attack plotters, leaves fewer dots for investigators to connect in time to stop an attack - and end-to-end and user-only-access encryption increasingly hide even those often precious few and fleeting dots.

In one instance, while planning and right up until the eve of the December 6, 2019 shooting at Naval Air Station Pensacola that killed three U.S. sailors and severely wounded eight other Americans, deceased terrorist Mohammed Saeed Al-Shamrani communicated undetected with overseas al-Qa'ida terrorists using an end-to-end encrypted app. Then, after the attack, user-only-access encryption prevented the FBI from accessing information contained in his phones for several months. As a result, during the critical time period immediately following the shooting and despite obtaining search warrants for the deceased killer's devices, the FBI could not access the information on those phones to identify co-conspirators, or determine whether they may have been plotting additional attacks.

This problem spans international and domestic terrorism threats. Like Al-Shamrani, the plotters who sought to kidnap the Governor of Michigan late last year used end-to-end encrypted apps to hide their communications from law enforcement. Their plot was only disrupted by well-timed human source reporting and the resulting undercover operation. Subjects of our investigation into the January 6 Capitol siege used end-to-end encrypted communications as well.

We face the same problem in protecting children against violent sexual exploitation. End-to-end and user-only-access encryption frequently prevent us from discovering and searching for victims, since the vital tips we receive from providers only arrive when those providers themselves are able to detect and report child exploitation being facilitated on their platforms and services. They cannot do that when their platforms are end-to-end encrypted. For example, while Facebook Messenger and Apple iMessage each boast over one billion users, in 2020, the National Center for Missing and Exploited Children ('NCMEC') received over 20 million tips from Facebook, compared to 265 tips from Apple, according to NCMEC data and publicly available information. Apple's use of end-to-end encryption, which blinds it to child sexual abuse material being transmitted through its services, likely plays a role in the disparities in reporting between the two companies. We do not know how many children are being harmed across the country as a result of this under-reporting, by Apple and other end-to-end providers.

When we are able to open investigations, end-to-end and user-only-access encryption makes it much more difficult to bring perpetrators to justice. Much evidence of crimes against children, just like many other kinds of crime today, exists primarily in electronic form. If we cannot obtain that critical electronic evidence, our efforts are frequently hamstrung.

This problem is not just limited to federal investigations. Our State and local law enforcement partners have been consistently advising the FBI that they, too, are experiencing similar end-to-end and user-only-access encryption challenges, which are now being felt across the full range of State and local crime. Many report that even relatively unsophisticated criminal groups, like street gangs, are frequently using user-only-access encrypted smartphones and end-to-end encrypted communications apps to shield their activities from detection or disruption. As this problem becomes more and more acute for State and local law enforcement, the advanced technical resources needed to address even a single investigation involving end-to-end and user-only-access encryption will continue to diminish and ultimately overwhelm State and local capacity to investigate even common crimes.

Cyber

In 2020, nation-state and criminal cyber actors took advantage of people and networks made more vulnerable by the sudden shift of our personal and professional lives online due to the COVID-19 pandemic, targeting those searching for personal protective equipment, worried about stimulus checks, and conducting vaccine research.

Throughout the last year, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cyber-criminal syndicates and nation-states keep innovating ways to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors as a way to access scores of victims by hacking just one provider.

These criminals and nation-states believe that they can compromise our networks, steal our property, and hold our critical infrastructure at risk without incurring any risk themselves. In the last year alone, we have seen - and have publicly called out - China, North Korea, and Russia for using cyber operations to target U.S. COVID-19 vaccines and research. We have seen the far-reaching disruptive impact a serious supply-chain compromise can have through the SolarWinds intrusions, which we believe was conducted by an Advanced Persistent Threat actor, likely Russian in origin. We have seen China working to obtain controlled defense technology and developing the ability to use cyber means to complement any future real-world conflict. We have seen Iran use cyber means to try to sow divisions and undermine our elections, targeting voters before the November election and threatening election officials after.

As dangerous as nation-states are, we do not have the luxury of focusing on them alone. In the past year, we also have seen cyber criminals target hospitals, medical centers, and educational institutions for theft or ransomware. Such attacks on medical centers have led to the interruption of computer networks and systems that put patients' lives at an increased risk at a time when America faces its most dire public health crisis in generations.

We are also seeing dark web vendors who sell capabilities in exchange for cryptocurrency increase the difficulty of stopping what would once have been less dangerous offenders. What was once a ring of unsophisticated criminals now has the tools to paralyze entire hospitals, police departments, and businesses with ransomware. It is not that individual hackers alone have necessarily become much more sophisticated, but - unlike previously - they are able to rent sophisticated capabilities.

We have to make it harder and more painful for hackers and criminals to do what they are doing. That is why I announced a new FBI cyber strategy last year, using the FBI's role as the lead federal agency with law enforcement and intelligence responsibilities to not only pursue our own actions, but to work seamlessly with our domestic and international partners to defend their networks, attribute malicious activity, sanction bad behavior, and take the fight to our adversaries overseas. We must impose consequences on cyber adversaries and use our collective law enforcement and intelligence capabilities to do so through joint and enabled operations sequenced for maximum impact. And we must continue to work with the Department of State and other key agencies to ensure that our foreign partners are able and willing to cooperate in our efforts to bring the perpetrators of cybercrime to justice.

An example of this approach is the international takedown in January 2021 of the Emotet botnet, which enabled a network of cyber criminals to cause hundreds of millions of dollars in damages to government, educational, and corporate networks. The FBI used sophisticated techniques, our unique legal authorities, and, most importantly, our worldwide partnerships to significantly disrupt the malware. We imposed upwards of 1,100 consequences on cyber adversaries last year, including arrests, criminal charges, convictions, dismantlements, and disruptions, and enabled many more actions through our dedicated partnerships with the private sector, foreign partners, and at the federal, State, and local level.

We have been putting a lot of energy and resources into all of those partnerships, especially with the private sector. We are working hard to push important threat information to network defenders, but we have also been making it as easy as possible for the private sector to share important information with us. For example, we are emphasizing to the private sector how we keep our presence unobtrusive in the wake of a breach; how we protect information that companies and universities share with us, and commit to providing useful feedback; and how we coordinate with our government partners so that we are speaking with one voice. But we need the private sector to do its part, too. We need the private sector to come forward to warn us -- and warn us quickly -- when they see malicious activity. We also need the private sector to work with us when we warn them that they are being targeted. The SolarWinds example only emphasizes what I have been saying for a long time: The government cannot protect against cyber threats on its own. We need a whole-of-society approach that matches the scope of the danger.

There is really no other option for defending a country where nearly all of our critical infrastructure, personal data, intellectual property, and network infrastructure sits in private hands.

Foreign Influence

Our nation is confronting multifaceted foreign threats seeking to both influence our national policies and public opinion, and cause harm to our national dialogue. The FBI and our interagency partners remain concerned about, and focused on, the covert and overt influence measures used by certain adversaries in their attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

Foreign influence operations - which include subversive, undeclared, coercive, and criminal actions by foreign governments to influence U.S. political sentiment or public discourse or interfere in our processes themselves - are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries - hoping to reach a wide swath of Americans covertly from outside the United States - to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, we established the Foreign Influence Task Force ('FITF') to identify and counteract malign foreign influence operations targeting the United States. The FITF is led by the Counterintelligence Division and is comprised of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States. In all instances, the FITF strives to protect democratic institutions; develop a common operating picture; raise adversaries' costs; and reduce their overall asymmetric advantage.

The FITF brings the FBI's national security and traditional criminal investigative expertise under one umbrella to prevent foreign influence in our elections. This better enables us to frame the threat, to identify connections across programs, to aggressively investigate as appropriate, and - importantly - to be more agile. Coordinating closely with our partners and leveraging relationships we have developed in the technology sector, we had a number of instances where we were able to quickly relay threat indicators that those companies used to take swift action, blocking budding abuse of their platforms.

Following the 2018 midterm elections, we reviewed the threat and the effectiveness of our coordination and outreach. As a result of this review, we further expanded the scope of the FITF. Previously, our efforts to combat malign foreign influence focused solely on the threat posed by Russia. Utilizing lessons learned over the last year and half, the FITF is widening its aperture to confront malign foreign operations of China, Iran, and other global adversaries. To address this expanding focus and wider set of adversaries and influence efforts, we have also added resources to maintain permanent 'surge' capability on election and foreign influence threats.

We have also further refined our strategy to ensure all efforts are based on a three-pronged approach, which includes investigations and operations, information and intelligence sharing, and a strong partnership with the private sector. Through the efforts of the FITF, and lessons learned from both the 2016 and 2018 elections, the FBI is actively engaged in identifying, detecting, and disrupting threats to our elections and ensuring both that the integrity of our democracy is preserved and that the will of the American people is fulfilled.

Conclusion

Finally, the strength of any organization is its people. The threats we face as a nation have never been greater or more diverse and the expectations placed on the FBI have never been higher. Our fellow citizens look to the FBI to protect the United States from all of those threats, and the men and women of the FBI continue to meet and exceed those expectations, every day. I want to thank them for their dedicated service.

Chairman Durbin, Ranking Member Grassley, and Members of the Committee, thank you for the opportunity to testify today. I am happy to answer any questions you might have.

Read this original document at: <https://www.judiciary.senate.gov/download/director-wray-testimony&download=1>

COMMITTEE TESTIMONY

March 2, 2021

Sen. Grassley,

Committee:

Senate Judiciary Committee

Subject:

FBI Oversight/Current Security Threats

Testimony:

Director Wray, thank you for being here today.

We all agree that what happened at the Capitol was a desecration of our shared values. It was an attack on the seat of democracy. Those who engaged in violence disgraced our country.

At least seven people, including one U.S. Capitol Police Officer, died as a result of that day. Two officers committed suicide, and hundreds were injured. May God watch over them and their families.

Those who broke the law must be prosecuted, and Congress needs answers, especially about what happened to Officer Brian Sicknick.

In pursuit of the facts relating to January 6, Senator Durbin and I have sent oversight letters to the FBI and other agencies. To date, we haven't received any productions. It's difficult to hold a hearing like this without records. The FBI must fully respond to Congress.

However, I'm pleased to see that many investigative cases are progressing around the country. As I've noted before, the ultimate responsibility for this attack rests upon the shoulders of those who unlawfully entered the Capitol. I've also made clear that everyone involved must take responsibility for their actions that day, including the former president.

Now, in the wake of January 6, we must seriously examine the threat of domestic extremism. But, unfortunately, this threat isn't limited to the events of that terrible day. To fully address it, we must examine forms of domestic extremism that span the ideological spectrum.

A narrow review of these matters would be intellectually dishonest.

We're not serious about tackling domestic extremism if we tolerate mobs that attack some police officers but not others.

We're not serious about tackling domestic extremism if we care about some government buildings being attacked but not others.

We're not serious about tackling domestic extremism if we only focus on white supremacy movements, which isn't the only ideology that's responsible for murders and violence.

Yes, white supremacy movements may be considered the most dangerous at a given time, but it wasn't last summer, or won't be when the next foreign attack is attempted. We must call it out across the board, left and right, every time. We must focus our resources to try to see as much of it coming as we possibly can.

It hardly registered in the media when Marshals and Secret Service officers defended courthouses and the White House. They were called 'stormtroopers' by the Speaker of the House, like they aren't even human beings. Vice President Harris, when she was a Senator, supported the Minnesota Freedom Fund, an organization that helped bail out violent rioters in Minnesota. 13 Biden staffers boasted on Twitter that they donated to the group. According to one news report, the group paid 75,000 dollars to get one man out of jail after he was charged with attempted murder for allegedly shooting at police during May protests.

One of the most upsetting aspects of the violence this summer has been the targeting of innocent law enforcement officers. More than 700 officers were injured between May 27, 2020, and June 8, 2020 alone.

Officers have been assaulted, slashed, struck with hammers and baseball bats, and blinded with lasers. Sixty Secret Service officers were injured during a three-day siege on the White House, which caused then-President Trump to be brought into a secure bunker. The church across the street was lit on fire as a part of that continued left-wing assault.

More than 300 people were charged federally for their roles in those months of violence. Eighty of those charges related to the use of arson and explosives. At least 14,000 people were arrested in 49 cities.

At least 25 people died in violence related to the riots.

There's been 280 arrests as a result of the January 6 attack compared to more than 1,000 arrests as a result of riots just in Portland last year. It's been estimated that the insurance losses from the summer's civil unrest possibly exceed 2 billion dollars.

It's been a relatively frequent sight at the summer's violent events to see individuals acting in coordination, holding the 'A' symbol of Antifa. An admitted Antifa adherent in Portland murdered a conservative protestor. Antifa supporters have been charged federally for promoting riots and using Molotov cocktails. Even after President Biden's electoral victory, Antifa rioters attacked the Oregon Democratic Party headquarters on Inauguration Day.

Let's not forget about the left-wing activist who opened fire on 24 Republican congressmen and hit a Capitol Police officer, a congressional aide, a lobbyist, and Rep. Steve Scalise at a baseball field in Alexandria, Virginia. Rep. Scalise had life-threatening injuries.

In light of these ever-present left-wing threats, I'm concerned about 'resource shifting' talk among Congressional Democrats.

Let me say this clearly: we aren't going to defund the anarchist extremism program or any other domestic terrorism program. It can't be that the FBI needs a fully funded Art Theft program but can't afford to fight both right-wing and left-wing extremism.

We must examine the issue of domestic terrorism broadly, to include the left and right wing of the political spectrum. No serious oversight activity and no serious policy decisions can be done without doing so.

As we move forward, I encourage both houses of Congress to review not just the events of January 6, but also domestic violent extremism across the board and the threat that it brings to our families and communities. We need real answers on extremist involvement, on pre-planning and coordination, and on what happened to Officer Sicknick.

In closing, I want to express my sincere thanks and appreciation for law enforcement and in particular, the Capitol Police, for their efforts on the job and during the terrible events of January 6. You are heroes.

Read this original document at: <https://www.judiciary.senate.gov/03/02/2021/grassley-statement&download=1>

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 131:

Combating Foreign Influence



Foreign influence operations—which include covert actions by foreign governments to influence U.S. political sentiment or public discourse—are not a new problem. But the interconnectedness of the modern world, combined with the anonymity of the Internet, have changed the nature of the threat and how the FBI and its partners must address it. The goal of these foreign influence operations directed against the United States is to spread disinformation, sow discord, and, ultimately, undermine confidence in our democratic institutions and values.

The FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, Director Christopher Wray established the Foreign Influence Task Force (FITF) to identify and counteract malign foreign influence operations targeting the United States.

Foreign influence operations have taken many forms and used many tactics over the years. Most widely reported these days are attempts by adversaries—hoping to reach a wide swath of Americans covertly from outside the United States—to use false personas and fabricated stories on social media platforms to discredit U.S. individuals and institutions.

Other influence operations by adversaries include:

- Targeting U.S. officials and other U.S. persons through traditional intelligence tradecraft
- Criminal efforts to suppress voting and provide illegal campaign financing
- Cyber attacks against voting infrastructure, along with computer intrusions targeting elected officials and others

The FITF is made up of representatives from our Counterintelligence, Cyber, Criminal, and Counterterrorism Divisions, and the task force also coordinates with other FBI divisions as needed. Task force personnel work closely with other U.S. government agencies and international partners concerned about foreign influence efforts aimed at their countries.

Through the FITF, the FBI is taking a three-pronged approach to this serious threat:

- *Investigations and operations:* The FITF works with FBI field offices across the country to counter the extensive influence operations of our foreign adversaries.
- *Information and intelligence sharing:* The FBI works closely with other intelligence community agencies, as well as with state and local law enforcement partners and election officials, to ensure a common understanding of the threat and a unified strategy to address it.
- *Private sector partnerships:* The FBI considers strategic engagement with U.S. technology companies, including threat indicator sharing, to be important in combating foreign influence actors.

Resources

- Protected Voices
- FBI Director Christopher Wray’s Statement at Press Briefing on Election Security
- Deputy Assistant Attorney General Adam S. Hickey’s Statement at Senate Judiciary Committee Hearing on Election Interference
- Security Resources for the Election Infrastructure Subsector (English, PDF)
 - Security Resources for the Election Infrastructure Subsector (Arabic, PDF)
 - Security Resources for the Election Infrastructure Subsector (Chinese, PDF)
 - Security Resources for the Election Infrastructure Subsector(French, PDF)
 - Security Resources for the Election Infrastructure Subsector (Spanish, PDF)
 - Security Resources for the Election Infrastructure Subsector (Tagalog, PDF)

Most Wanted

- Ten Most Wanted
- Fugitives
- Terrorism
- Kidnappings / Missing Persons
- Seeking Information
- Bank Robbers
- ECAP
- ViCAP

News

- Stories
- Videos
- Press Releases
- Speeches
- Testimony
- Podcasts and Radio
- Photos
- Español

What We Investigate

- Terrorism
- Counterintelligence
- Cyber Crime
- Public Corruption
- Civil Rights
- Organized Crime
- White-Collar Crime
- Violent Crime

Contact Us

- Field Offices
- FBI Headquarters
- Overseas Offices
- Additional Resources
- Accessibility
- eRulemaking

DEFENDANTS' EXHIBIT 132:

2020 WL 996966 (D.O.J.)

Department of Justice (D.O.J.)

Federal Bureau of Investigation (FBI)

(NEWS RELEASE)

JOINT STATEMENT FROM DOS, DOJ, DOD, DHS, ODNI, FBI,
NSA, AND CISA ON PREPARATIONS FOR SUPER TUESDAY

March 2, 2020

Secretary of State Mike Pompeo, U.S. Attorney General William Barr, Secretary of Defense Mark Esper, Acting Secretary of Homeland Security Chad Wolf, Acting Director of National Intelligence Richard Grenell, Federal Bureau of Investigation Director Christopher Wray, U.S. Cyber Command Commander and National Security Agency Director Gen. Paul Nakasone, and Cybersecurity and Infrastructure Security Agency Director Christopher Krebs today released the following joint statement:

Tomorrow, millions of voters in more than a dozen states and territories will cast their votes in presidential primaries. ‘Super Tuesday’ will see more Americans head to the polls than any other day of the primary season. We continue to work with all 50 states, U.S. territories, local officials, political parties, and private sector partners to keep elections free from foreign interference.

Americans must also remain aware that foreign actors continue to try to influence public sentiment and shape voter perceptions. They spread false information and propaganda about political processes and candidates on social media in hopes to cause confusion and create doubt in our system. We remain alert and ready to respond to any efforts to disrupt the 2020 elections. We continue to make it clear to foreign actors that any effort to undermine our democratic processes will be met with sharp consequences.

The level of coordination and communication between the federal government and state, local, and private sector partners is stronger than it's ever been. Our departments and agencies are working together in an unprecedented level of commitment and effort to protect our elections and to counter malign foreign influence, but voters have a role to play too.

We encourage all voters going to the polls to check your voter registration and know ahead of time when to vote, where to vote, what's on your ballot, and whether your state requires identification. Your state or local election official's office is the most trusted source for election material. A well-informed and vigilant republic is the best defense against disinformation.

Washington, D.C.
FBI National Press Office
(202) 324-3691

2020 WL 996966 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 133:

2020 WL 5644950 (D.O.J.)

Department of Justice (D.O.J.)

Federal Bureau of Investigation (FBI)

(NEWS RELEASE)

**FOREIGN ACTORS AND CYBERCRIMINALS LIKELY TO SPREAD
DISINFORMATION REGARDING 2020 ELECTION RESULTS**

September 22, 2020

The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) are issuing this announcement to raise awareness of the potential threat posed by attempts to spread disinformation regarding the results of the 2020 elections. Foreign actors and cybercriminals could create new websites, change existing websites, and create or share corresponding social media content to spread false information in an attempt to discredit the electoral process and undermine confidence in U.S. democratic institutions.

State and local officials typically require several days to weeks to certify elections' final results in order to ensure every legally cast vote is accurately counted. The increased use of mail-in ballots due to COVID-19 protocols could leave officials with incomplete results on election night. Foreign actors and cybercriminals could exploit the time required to certify and announce elections' results by disseminating disinformation that includes reports of voter suppression, cyberattacks targeting election infrastructure, voter or ballot fraud, and other problems intended to convince the public of the elections' illegitimacy.

The FBI and CISA urge the American public to critically evaluate the sources of the information they consume and to seek out reliable and verified information from trusted sources, such as state and local election officials. The public should also be aware that if foreign actors or cyber criminals were able to successfully change an election-related website, the underlying data and internal systems would remain uncompromised.

RECOMMENDATIONS

- * Seek out information from trustworthy sources, such as state and local election officials; verify who produced the content; and consider their intent.
- * Verify through multiple reliable sources any reports about problems in voting or election results, and consider searching for other reliable sources before sharing such information via social media or other avenues.
- * For information about final election results, rely on state and local government election officials.
- * Report potential election crimes--such as disinformation about the manner, time, or place of voting--to the FBI.
- * If appropriate, make use of in-platform tools offered by social media companies for reporting suspicious posts that appear to be spreading false or inconsistent information about election-related problems or results.

The FBI is responsible for investigating malign foreign influence operations and malicious cyber activity targeting election infrastructure and other U.S. democratic institutions. CISA is responsible for protecting the nation's critical infrastructure from physical and cyber threats. The FBI and CISA provide services and information to uphold the security, integrity, and resiliency of the U.S. electoral processes.

VICTIM REPORTING AND ADDITIONAL INFORMATION

The FBI encourages victims to report information concerning suspicious or criminal activity to their local field office (www.fbi.gov/contact-us/field). For additional assistance and best practices, and common terms, please visit the following websites:

- * Protected Voices: www.fbi.gov/investigate/counterintelligence/foreign-influence/protected-voices
- * Election Crimes and Security: www.fbi.gov/scams-and-safety/common-scams-and-crimes/election-crimes-and-security
- * #Protect2020: www.cisa.gov/protect2020

2020 WL 5644950 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 134:

NewsRoom

4/24/23 WashingtonPost.com (Pg. Unavail. Online)
2023 WLNR 14537844

WashingtonPost.com
Copyright (c) 2023 The Washington Post

April 24, 2023

Section: /technology/tech-policy

Iran gained access to election results website in 2020, military reveals

Joseph Menn

SAN FRANCISCO — The U.S. military discovered that an Iranian hacking group had penetrated a local government website that was to report 2020 election results and disrupted the attack before the votes were tallied, officials revealed Monday during a conference of cybersecurity professionals.

Officials said that while neither the votes nor the counting machines would have been affected by the intrusion, the hackers could have rendered the public-facing website for displaying results unreachable or posted fake results, shaking public confidence in the true results.

"It could make it look like the votes had been tampered with," said Maj. Gen. William J. Hartman, commander of the Cyber Command's Cyber National Mission Force.

Hartman did not reveal which website had been penetrated. He said his group of 2,000 cyber experts discovered the penetration during its "hunt forward" efforts overseas, then alerted the Department of Homeland Security, which helped the unnamed local government thwart the intrusion.

Hartman spoke during a rare joint presentation with the head of the DHS agency for domestic cyberdefense at the annual RSA security industry conference in San Francisco. Until his presentation Monday, the Iranian intrusion had been classified.

The talk with Eric Goldstein, leader for cybersecurity at the Cybersecurity and Infrastructure Security Agency (CISA), was intended to stress the ongoing and rapid cooperation between the two agencies against spies, ransomware operators and potentially destructive hackers.

Hartman said the Iranian group was known in the industry as Pioneer Kitten, after the private company CrowdStrike's term for a suspected Iranian government contractor. He said it was a distinct operation from another 2020 Iranian disruption attempt in which faked emails supposedly from the militant far-right Proud Boys threatened voters if they didn't support Donald Trump.

Another detail declassified for Monday's presentation concerned the sophisticated and pervasive hacks in 2020 of software from SolarWinds and Microsoft, in which alleged Russian government hackers burrowed deep inside SolarWinds' process for generating final programming code. The impact of the SolarWinds hack was particularly widespread because the company held

contracts to update the computers of scores of businesses and government agencies, including the Commerce and Treasury departments.

After experts at Mandiant detected the attack on the security firm's own copy of SolarWinds, CISA went to that company and made an electronic copy of its infected server, Goldstein said. Cyber Command then trained its troops on that electronic image, and the practice helped them hunt the programmers behind it, eventually discovering 18 other malicious programs from the same team, which Hartman said was part of Russia's SVR foreign intelligence agency.

The breaches reached into nine U.S. government agencies, but Goldstein said all were confident they had fully evicted the intruders.

Hartman said the collaboration between Cyber Command and CISA is more extensive than most people realize and that some senior executives and front-line analysts from each agency are physically located at the other agency.

Speaking to reporters after the session, Hartman said his force has undertaken 47 forward operations in the past three years, with teams ranging in size from 10 members to the 43 currently deployed in Ukraine.

Feeding information that those teams have discovered in the field back to CISA has helped the domestic agency warn 160 targets just this year that they were about to be ransomware victims, Goldstein said.

Hartman also disclosed for the first time that Cyber Command had cut off suspected Chinese hackers from access to hundreds of infected Microsoft Exchange email servers in 2021.

The RSA conference takes its name from the RSA security company that began it. The letters come from the last names of RSA founders Ron Rivest, Adi Shamir and Leonard Adleman, all cryptography experts. The company is now owned by Dell EMC.

Tim Starks contributed to this report.

---- Index References ----

Company: CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY; EMC CORPORATION; MICROSOFT CORPORATION; CROWDSTRIKE HOLDINGS, INC.

News Subject: (Consumer Protection (1CO43); Data Privacy & Protection (1DA12); Emerging Market Countries (1EM65); Legal (1LE33))

Industry: (Homeland Security (1HO11); Internet (1IN27); Internet Regulatory (1IN49); Internet Security (1IN07); Security (1SE29); Security Software (1SE53))

Region: (Asia (1AS61); CIS Countries (1CI64); Eastern Europe (1EA48); Europe (1EU83); Gulf States (1GU47); Iran (1IR40); Middle East (1MI23); Russia (1RU33); Western Asia (1WE54))

Language: EN

Other Indexing: (Iran; Cyber National Mission Force; Department of Homeland Security; Pioneer Kitten; RSA; Cybersecurity and Infrastructure Security Agency; Dell EMC; Microsoft; CrowdStrike)

Word Count: 618

NewsRoom

DEFENDANTS' EXHIBIT 135:

DOJ 18-923 (D.O.J.), 2018 WL 3425704

Department of Justice (D.O.J.)

Deputy Attorney General (DAG)

(NEWS RELEASE)

**GRAND JURY INDICTS 12 RUSSIAN INTELLIGENCE OFFICERS
FOR HACKING OFFENSES RELATED TO THE 2016 ELECTION**

July 13, 2018

The Department of Justice today announced that a grand jury in the District of Columbia returned an indictment presented by the Special Counsel's Office. The indictment charges twelve Russian nationals for committing federal crimes that were intended to interfere with the 2016 U.S. presidential election. All twelve defendants are members of the GRU, a Russian Federation intelligence agency within the Main Intelligence Directorate of the Russian military. These GRU officers, in their official capacities, engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton, and released that information on the internet under the names "DCLeaks" and "Guccifer 2.0" and through another entity.

"The Internet allows foreign adversaries to attack America in new and unexpected ways," said Deputy Attorney General Rod J. Rosenstein. "Together with our law enforcement partners, the Department of Justice is resolute in its commitment to locate, identify and seek to bring to justice anyone who interferes with American elections. Free and fair elections are hard-fought and contentious, and there will always be adversaries who work to exacerbate domestic differences and try to confuse, divide, and conquer us. So long as we are united in our commitment to the shared values enshrined in the Constitution, they will not succeed."

According to the allegations in the indictment, Viktor Borisovich Netyksho, Boris Alekseyevich Antonov, Dmitriy Sergeyevich Badin, Ivan Sergeyevich Yermakov, Aleksey Viktorovich Lukashev, Sergey Aleksandrovich Morgachev, Nikolay Yuryevich Kozachek, Pavel Vyacheslavovich Yershov, Artem Andreyevich Malyshev, Aleksandr Vladimirovich Osadchuk, Aleksey Aleksandrovich Potemkin, and Anatoliy Sergeyevich Kovalev were officials in Unit 26165 and Unit 74455 of the Russian government's Main Intelligence Directorate.

In 2016, officials in Unit 26165 began spearphishing volunteers and employees of the presidential campaign of Hillary Clinton, including the campaign's chairman. Through that process, officials in this unit were able to steal the usernames and passwords for numerous individuals and use those credentials to steal email content and hack into other computers. They also were able to hack into the computer networks of the Democratic Congressional Campaign Committee (DCCC) and the Democratic National Committee (DNC) through these spearphishing techniques to steal emails and documents, covertly monitor the computer activity of dozens of employees, and implant hundreds of files of malicious computer code to steal passwords and maintain access to these networks.

The officials in Unit 26165 coordinated with officials in Unit 74455 to plan the release of the stolen documents for the purpose of interfering with the 2016 presidential election. Defendants registered the domain DCLeaks.com and later staged the release of thousands of stolen emails and documents through that website. On the website, defendants claimed to be "American hacktivists" and used Facebook accounts with fictitious names and Twitter accounts to promote the website. After public accusations that the Russian government was behind the hacking of DNC and DCCC computers, defendants created the fictitious persona Guccifer 2.0. On the evening of June 15, 2016 between 4:19PM and 4:56PM, defendants used their Moscow-based server to search for a series of English words and phrases that later appeared in Guccifer 2.0's first blog post falsely claiming to be a lone Romanian hacker responsible for the hacks in the hopes of undermining the allegations of Russian involvement.

Members of Unit 74455 also conspired to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections to steal voter data stored on those computers.

To avoid detection, defendants used false identities while using a network of computers located around the world, including the United States, paid for with cryptocurrency through mining bitcoin and other means intended to obscure the origin of the funds. This funding structure supported their efforts to buy key accounts, servers, and domains. For example, the same bitcoin mining operation that funded the registration payment for DCLeaks.com also funded the servers and domains used in the spearphishing campaign.

The indictment includes 11 criminal counts:

- * Count One alleges a criminal conspiracy to commit an offense against the United States through cyber operations by the GRU that involved the staged release of stolen documents for the purpose of interfering with the 2016 president election;
- * Counts Two through Nine charge aggravated identity theft for using identification belonging to eight victims to further their computer fraud scheme;
- * Count Ten alleges a conspiracy to launder money in which the defendants laundered the equivalent of more than \$95,000 by transferring the money that they used to purchase servers and to fund other costs related to their hacking activities through cryptocurrencies such as bitcoin; and
- * Count Eleven charges conspiracy to commit an offense against the United States by attempting to hack into the computers of state boards of elections, secretaries of state, and US companies that supplied software and other technology related to the administration of elections.

There is no allegation in the indictment that any American was a knowing participant in the alleged unlawful activity or knew they were communicating with Russian intelligence officers. There is no allegation in the indictment that the charged conduct altered the vote count or changed the outcome of the 2016 election.

Everyone charged with a crime is presumed innocent unless proven guilty in court. At trial, prosecutors must introduce credible evidence that is sufficient to prove each defendant guilty beyond a reasonable doubt, to the unanimous satisfaction of a jury of twelve citizens.

This case was investigated with the help of the FBI's cyber teams in Pittsburgh, Philadelphia and San Francisco and the National Security Division. The Special Counsel's investigation is ongoing. There will be no comments from the Special Counsel at this time.

DOJ 18-923 (D.O.J.), 2018 WL 3425704

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 136:

Hawley Calls for FEC Investigation of Potential In-Kind Contributions from Twitter and Facebook to Biden Campaign

Wednesday, October 14, 2020

Today U.S. Senator Josh Hawley (R-Mo.) wrote a letter (</sites/default/files/2020-10/Hawley-Letter-to-FEC-Biden-New-York-Post-Twitter-Facebook.pdf>) to the Federal Election Commission (FEC) General Counsel expressing serious concerns about the possibility of campaign finance violations benefitting the Biden campaign in Twitter and Facebook's suppression of the New York Post's reporting on Hunter Biden. Senator Hawley writes that, as the Biden campaign derives value from the suppression of the story, the companies may have therefore made in-kind contributions to the campaign.

Senator Hawley writes, "These possible campaign-finance violations by two of the most powerful corporations in America comes only weeks before Election Day, and while millions of Americans are in the midst of voting. I ask that the FEC take immediate action to investigate these potential violations and, if appropriate, take remedial action to prevent further interference with the 2020 Presidential election."

Senator Hawley has also today written letters to Facebook (</hawley-demands-answers-facebook-over-censorship-hunter-biden-article>) and Twitter (</hawley-questions-dorsey-over-twitter-blackout-hunter-biden-story>) demanding answers regarding their censorship of the story.

Read the full letter here (</sites/default/files/2020-10/Hawley-Letter-to-FEC-Biden-New-York-Post-Twitter-Facebook.pdf>) or below.

October 14, 2020

Lisa J. Stevenson
Acting General Counsel
Federal Election Commission
Office of General Counsel
1050 First Street, NE
Washington, DC 20463

Dear Ms. Stevenson:

I write to express serious concern about the possibility that egregious campaign-finance violations benefitting the Biden campaign may be playing out in real time, just weeks before the presidential election. Earlier today, the New York Post published a bombshell report that Hunter Biden facilitated a meeting between a Ukrainian energy executive and his father, who was then Vice President. The Post article cites evidence that would directly contradict Joe Biden's claim that he has "never spoken to my son about his overseas business dealings."

The Post's reporting has understandably attracted substantial public discussion. And countless Americans have sought to discuss and debate that article via the forums in which so much of our political speech occurs: on social media. But two social-media platforms have engaged in unprecedented suppression of public discussion of the article. Twitter is blocking all tweets and direct messages that contain the URL for the Post article. Facebook has stated that it is "reducing [the story's] distribution on our platform," though the specifics of how Facebook will implement this remain opaque.

This conduct does not merely censor the core political speech of ordinary Americans, though it certainly does that. Twitter's and Facebook's conduct also appears to constitute a clear violation of federal campaign-finance law. Federal law prohibits any corporation from making a contribution to a federal candidate for office. 52 U.S.C. § 30118(a). Twitter and Facebook are both corporations. A "contribution" includes "anything of value . . . for the purpose of influencing any election for Federal office." 52 U.S.C. § 30101(8)(A)(i). Twitter's

and Facebook's active suppression of public speech about the New York Post article appears to constitute contributions under federal law. There can be no serious doubt that the Biden campaign derives extraordinary value from depriving voters access to information that, if true, would link the former Vice President to corrupt Ukrainian oligarchs. And this censorship manifestly will influence the presidential election.

These possible campaign-finance violations by two of the most powerful corporations in America comes only weeks before Election Day, and while millions of Americans are in the midst of voting. I ask that the FEC take immediate action to investigate these potential violations and, if appropriate, take remedial action to prevent further interference with the 2020 presidential election.

Sincerely,

Josh Hawley

United States Senator

Issues

Big Tech (/issues/big-tech)

< PREVIOUS (/HAWLEY-QUESTIONS-DORSEY-OVER-TWITTER-BLACKOUT-HUNTER-BIDEN-STORY) NEXT > (/FOLLOWING-POTENTIAL-CAMPAIGN-FINANCE-VIOLATION-HAWLEY-CALL-FACEBOOK-TWITTER-CEOS-TESTIFY-REGARDING)

Sign up for Updates

First Name *

Last Name *

Email *

Subscribe



(<https://www.facebook.com/SenatorHawley/>)



(<https://twitter.com/SenHawleyPress>)



(https://www.youtube.com/channel/UCMzt8xq6qQ3XQ_DLnfJx0-w)



(<https://www.instagram.com/senatorhawley/>)

Cape Girardeau

555 Independence Street, #1600
Cape Girardeau, MO 63703
Office: 573-334-5995
Fax: 573-334-5947

Columbia

1123 Wilkes Blvd, Suite 220
Columbia, MO 65201
Office: 573-554-1919
Fax: 573-256-1805

Kansas City

400 E. 9th Street, Suite 9350

Kansas City, MO 64106

Office: 816-960-4694

Fax: 816-472-6812

Springfield

901 E. St. Louis Street, Suite 1604

Springfield, MO 65806

Office: 417-869-4433

Fax: 417-869-4411

St. Louis

111 South 10th Street, Suite 23.360

St. Louis, MO 63102

Office: 314-354-7060

Fax: 1 314-436-8534

Washington, D.C.

115 Russell Senate Office Building

Washington, D.C. 20510

Office: 202-224-6154

Fax: 202-228-0526

DEFENDANTS' EXHIBIT 137:

2020 WL 13568471
Bloomberg Government
Copyright (c) 2020 Bloomberg Government

Testimony
November 17, 2020

Committee on the Judiciary

Committee Hearing Censorship/Suppression and the 2020 Election

CQ Abstract

Committee:

Senate Judiciary Committee

Subject:

Censorship/Suppression and the 2020 Election

Abstract:

Senate Judiciary Committee (Chairman Lindsey Graham, R-S.C.) hearing on ‘Breaking the News: Censorship, Suppression, and the 2020 Election.’

Scheduled Witnesses:

Facebook CEO Mark Zuckerberg

Twitter CEO Jack Dorsey testify

COMMITTEE TESTIMONY

Nov. 17, 2020

Mark Zuckerberg, Chief Executive Officer, Facebook, Inc., Menlo Park, CA

Committee:

Senate Judiciary Committee

Subject:

Censorship/Suppression and the 2020 Election

Testimony:

I. Introduction

Chairman Graham, Ranking Member Feinstein, and members of the Committee, thank you for the opportunity to be here today.

Facebook's mission is to give people the power to build community and bring the world closer together. Our products enable more than 3 billion people around the world to share ideas, offer support, and discuss important issues, including politics, public health, and social issues. We think that community is particularly important now when the COVID-19 pandemic has disrupted so many aspects of our daily lives. We believe we have a responsibility to keep people safe on our service and to protect free expression, and we work hard to set and enforce policies that meet this goal.

II. Our Efforts to Support the 2020 Election

Facebook stands for giving people a voice, and it was important to us that everyone could make their voice heard during the election. While we were only a small piece of the broader election ecosystem, we announced a series of policies in advance to help protect the integrity of the election and support our democratic process.

First, we proactively supported civic engagement on our platform. We ran the largest voting information campaign in American history. Based on conversion rates we calculated from a few states we partnered with, we estimate that we helped 4.5 million people register to vote across Facebook, Instagram, and Messenger--and helped about 100,000 people sign up to be poll workers. We launched a Voting Information Center to connect people with reliable information on deadlines for registering and voting and details about how to vote by mail or vote early in person, and we displayed links to the Voting Information Center when people posted about voting on Facebook. 140 million people visited the Voting Information Center on Facebook and Instagram since it launched. We are encouraged that more Americans voted in 2020 than ever before, and that our platform helped people take part in the democratic process.

Second, we worked hard to tackle misinformation and voter suppression. People tell us they don't want to see misinformation on Facebook, and neither do we. We partnered with election officials to remove false claims about polling conditions and displayed warnings on more than 150 million pieces of content after review by our independent third-party fact-checkers. We put in place strong voter suppression policies prohibiting explicit or implicit misrepresentations about how or when to vote as well as attempts to use threats related to COVID-19 to scare people into not voting. We also removed calls for people to engage in poll watching that used militarized language or suggested that the goal was to intimidate, exert control, or display power over election officials or voters, and we filtered civic groups out of recommendations.

As the ballots were counted, we deployed additional measures that we announced in advance of the election to help people stay informed:

- * We partnered with Reuters and the National Election Pool to provide reliable information about election results in the Voting Information Center and notified people proactively as results became available. We added labels to posts about voting by candidates from both parties to direct people to reliable information.

- * We attached an informational label to content that sought to delegitimize the outcome of the election or discuss the legitimacy of voting methods.

- * We strengthened our enforcement against militias, conspiracy networks, and other groups to help prevent them from using our platform to organize violence or civil unrest in the period after the election. We have already removed thousands of these groups from our platform, and we will continue our enforcement during this transitional period.

Based on what we learned in 2016 about the risk of coordinated online efforts by foreign governments and individuals to interfere in our elections, we invested heavily in our security systems and monitored closely for any threats to the integrity of the

election from abroad. We also blocked ads from state-controlled media outlets in the US to provide an extra layer of protection against various types of foreign influence in the public debate ahead of the election.

We're pleased that, thanks to the hard work of election administrators across the country, the voting process went relatively smoothly. We expect there is still a lot to learn from this election, and we're committed to making sure that we do. Earlier this year, we announced a partnership with a team of independent external academics to conduct objective and empirically grounded research on social media's impact on democracy. We want to better understand whether social media makes us more polarized as a society, or if it largely reflects the divisions that already exist; if it helps people become more informed about politics, or less; or if it affects people's attitudes towards government and democracy, including whether and how they vote. We hope that the insights these researchers develop will help advance society's understanding of the intersection of technology and democracy and help Facebook learn how we can better play our part.

III. Updating the Rules of the Internet

We're committed to doing everything we can to protect our community while supporting free expression and democracy, but as I've said before, we don't think that tech companies should be making so many decisions about these important issues alone. I believe we need a more active role for governments and regulators, which is why, in March last year, I called for regulation on privacy, elections, and data portability.

I've also called for Congress to update Section 230 of the Communications Decency Act to make sure it's working as intended. Section 230 allows us to provide our products and services to users by doing two things:

- * First, it encourages free expression. Without Section 230, platforms could potentially be held liable for everything people say. Platforms would likely censor more content to avoid legal risk and would be less likely to invest in technologies that enable people to express themselves in new ways.

- * Second, it allows platforms to moderate content. Without Section 230, platforms could face liability for doing even basic moderation, such as removing hate speech and harassment that impacts the safety and security of their communities.

Thanks to Section 230, people have the freedom to use the internet to express themselves, and platforms are able to more effectively address risks. Updating Section 230 is a significant decision, but we support the ideas around transparency and industry collaboration that are being discussed in some of the current bipartisan proposals, and I look forward to a meaningful dialogue about how we might update the law to deal with the problems we face today.

It's important that any changes to the law don't prevent new companies or businesses from being built, because innovation in the internet sector brings real benefits to billions of people around the world. We stand ready to work with Congress on what regulation could look like, whether that means Section 230 reform or providing guidance to platforms on other issues such as harmful content, privacy, elections, and data portability. By updating the rules for the internet, we can preserve what's best about it--the freedom for people to express themselves and for entrepreneurs to build new things--while also protecting society from broader harms.

IV. Conclusion

We took our responsibility for protecting the integrity of this election seriously. We followed the policies and processes that we laid out in advance to protect the democratic process in both the pre- and post-election period, and we worked hard to apply those policies fairly and consistently.

Securing the integrity of elections is an ongoing challenge for platforms, and we are committed to continuing to improve our systems, but I am proud of the work we have done over the past four years to prevent election interference and support our

democracy. Millions of Americans used our service to talk about the campaigns, access credible information about voting, and register to vote.

At Facebook, we often have to balance competing equities. Sometimes the right thing to do from a safety or security perspective isn't the best for privacy or free expression, so we have to choose what we believe is best for our community and for the world. Making these tradeoffs is not straightforward, and whatever path we choose, inevitably some people are disappointed.

In addition, people have very different ideas about how the internet should be governed. This is something many platforms struggle with, and it's why I believe we should resolve some of these tensions together as a society and in a way that people feel is legitimate. We hope to work with both parties on regulation in the next Congress, and I look forward to discussing this at the hearing.

Read this original document at: <https://www.judiciary.senate.gov/download/zuckerberg-testimony&download=1>

COMMITTEE TESTIMONY

Nov. 17, 2020

Jack Dorsey, Chief Executive Officer, Twitter, Inc., San Francisco, CA

Committee:

Senate Judiciary Committee

Subject:

Censorship/Suppression and the 2020 Election

Testimony:

Chairman Graham, Ranking Member Feinstein, and Members of the Committee:

Thank you for the opportunity today to speak to the Committee and to the American people.

Twitter's purpose is to serve the public conversation. People from around the world come together on Twitter in an open and free exchange of ideas. We want to make sure conversations on Twitter are healthy and that people feel safe in expressing their points of view. We do our work with the recognition that free speech and safety are interconnected.

Today's hearing, Breaking the News: Censorship, Suppression, and the 2020 Election, was called, in part, as a response to enforcement decisions relating to Tweets by @NYPost on October 14, 2020, and concerns of this Committee regarding 'Big Tech,' censorship, and competition. The @NYPost example demonstrates the complexity of content moderation and policy enforcement decisions. The world has changed since Section 230 of the Communications Decency Act of 1996 became law, but the fundamentals of online speech that led to its passage largely remain.

Knowing that overly burdensome government regulatory schemes are not always nimble nor quick and can have unintended consequences, I encourage Congress to work with industry and civil society to build upon Section 230's foundation, whether it be through additions to Section 230, industry-wide self-regulation best practices, or a new legislative framework. By doing so, we can build an adaptable future Internet that people trust by empowering technology companies to continually make necessary changes to policies, services, and products, as well as experiment and learn, to improve their platforms and services.

Working together we can also avoid potential pitfalls. For example, completely eliminating Section 230 or prescribing reactionary government speech mandates will neither address concerns nor align with the First Amendment. Indeed, such actions could have the opposite effect, likely resulting in increased removal of speech, the proliferation of frivolous lawsuits, and severe limitations on our collective ability to address harmful content and protect people online.

Likewise, amending the law solely through carve-outs will inevitably favor large incumbents with vast resources who may willingly embrace such changes as it would leave only a small number of giant and well-funded technology companies. For innovation to thrive, we must not entrench the largest companies further.

The challenges that technology companies face on the Internet continue to change, requiring us to be agile in updating our policies and also make unprecedented investments to safeguard the public conversation. I would like to share what Twitter is doing to address your concerns and earn trust from those who use our services, which may help create a blueprint of solutions for the broader technology community. We also have taken steps to respond to an increasing demand from our consumers to provide context around misinformation - including our efforts around civic integrity and combating efforts to undermine the US 2020 election, which I will discuss today.

Building & Earning Trust

Three weeks ago, I told the Senate Committee on Commerce, Science and Transportation that I believe the best way to address our mutually-held concerns is to require the publication of moderation processes and practices, a straightforward process to appeal decisions, and best efforts around algorithmic choice, while protecting the privacy of the people who use our service. These are achievable in short order.

Transparency

We believe increased transparency is the foundation to promote healthy public conversation on Twitter and to earn trust. It is critical that people understand our processes and that we are transparent about what happens as a result. Content moderation rules and their potential effects, as well as the process used to enforce those rules, should be simply explained and understandable by everyone. We believe that companies like Twitter should publish their moderation process. We should be transparent about how cases are reported and reviewed, how decisions are made, and what tools are used to enforce. Publishing answers to questions like these will make our process more robust and accountable to the people we serve.

At Twitter, we use a combination of machine learning and humans to review reports and determine whether they violate the Twitter Rules. We take a behavior-first approach, meaning we look at how accounts behave before we review the content they are posting. Twitter's open nature means our enforcement actions are plainly visible to the public, even when we cannot reveal the private details of individual accounts that have violated our Rules. We have worked to build better in-app notices where we have removed Tweets for breaking our Rules. We also communicate with both the account that reports a Tweet and the account that posted it with additional detail on our actions. That said, we know we can continue to improve to further earn the trust of the people using Twitter.

We also know that an important part of transparency is acknowledging when our policies require updating because of new or unanticipated circumstances and acting quickly to make the necessary changes. The @NYPost situation is a prime example of this. In 2018, we created a policy to prevent Twitter from being used to spread hacked materials. This policy was informed by conversations with the US government about foreign state misinformation and disinformation and the use of hacked materials or materials of dubious origin being used to manipulate the electorate and influence the outcome of an election. These warnings from government partners were also repeated in advance of the 2018 US Midterm Election and 2020 US Election.

It was against this backdrop that we enforced our Hacked Materials Policy against very specific content shared by the @NYPost. Under this policy, people on Twitter were blocked from sharing certain links from the @NYPost, publicly or privately, as those specific articles contained the source materials themselves. References to the contents of the materials or discussion about the materials were not restricted under the policy. After hearing from journalists and others, we quickly updated our policy to limit its scope to only cover the removal of materials shared by hackers directly. This action, however, did not allow us to reinstate the @NYPost Tweets as we do not retroactively review enforcement actions when we update our policies. In order to address the unique facts in the @NYPost case, we determined that we should change our practices to allow for circumstances when actions on a specific account have led to a policy change. Accordingly, we updated the relevant policy, informed @NYPost, and the newspaper's account was restored. While we may have taken longer than some would have wanted to take these actions, we believe that this process and associated review have helped us create strong and more transparent policies.

Advancing Procedural Fairness

As a company, Twitter is focused on advancing the principle of procedural fairness in our decision-making across the board. We strive to give people an easy, clear way to appeal decisions we make that they think are not right. Mistakes in enforcement -- made either by a human or algorithm -- are inevitable, and why we strive to make appeals easier. We believe that all companies should be required to provide a straightforward process to appeal decisions. This makes certain people can let us know when we do not get it right, so that we can fix any mistakes and make our processes better in the future.

Procedural fairness at Twitter also means we ensure that all decisions are made without using political viewpoints, party affiliation, or political ideology, whether related to automatically ranking content on our service or how we develop or enforce the Twitter Rules. Our Twitter Rules are not based on ideology or a particular set of beliefs. We believe strongly in being impartial, and we strive to enforce our Twitter Rules fairly.

Algorithmic Choice

We believe that people should have choices about the key algorithms that affect their experience online. At Twitter, we want to provide a useful, relevant experience to all people using our service. With hundreds of millions of Tweets every day on Twitter, we have invested heavily in building systems that organize content to show individuals the most relevant information for that individual first. With 187 million people last quarter using Twitter each day in dozens of languages and countless cultural contexts, we rely upon machine learning algorithms to help us organize content by relevance.

In December 2018, Twitter introduced an icon located at the top of everyone's timelines that allows individuals using Twitter to easily switch to a reverse chronological order ranking of the Tweets from accounts or topics they follow. This improvement gives people more control over the content they see, and it also provides greater transparency into how our algorithms affect what they see. It is a good start. We believe this points to an exciting, market-driven approach where people can choose what algorithms filter their content so they can have the experience they want. We are inspired by the approach suggested by Dr. Stephen Wolfram, Founder and Chief Executive Officer of Wolfram Research, in his testimony before the Senate Committee on Commerce, Science and Transportation Subcommittee on Communications, Technology, Innovation, and the Internet in June 2019. Enabling people to choose algorithms created by third parties to rank and filter their content is an incredibly energizing idea that is within reach.

We also recognize that we can do even more to improve to provide greater algorithmic transparency and fair machine learning. The machine learning teams at Twitter are studying these techniques and developing a roadmap to ensure our present and algorithmic models uphold a high standard when it comes to transparency and fairness. We believe this is an important step in ensuring fairness in how we operate and we also know that it is critical that we be more transparent about our efforts in this space.

Protecting Privacy

In addition to the principles I have outlined to address content moderation issues in order to better serve consumers, it is also critical to protect the privacy of the people who use online services. We believe privacy is a fundamental human right, not a privilege. We offer a range of ways for people to control their privacy experience on Twitter, from offering pseudonymous accounts to letting people control who sees their Tweets to providing a wide array of granular privacy controls. Our privacy efforts have enabled people around the world using Twitter to protect their own data.

That same philosophy guides how we work to protect the data people share with Twitter. We empower the people who use our service to make informed decisions about the data they share with us. We believe individuals should know, and have meaningful control over, what data is being collected about them, how it is used, and when it is shared.

We believe that individuals should control the personal data that is shared with companies and provide them with the tools to help them control their data. Through the account settings on Twitter, we give people the ability to make a variety of choices about their data privacy, including limiting the data we collect, determining whether they see interest-based advertising, and controlling how we personalize their experience. In addition, we provide them with the ability to access information about advertisers that have included them in tailored audiences to serve them ads, demographic and interest data about their account from ad partners, and information Twitter has inferred about them.

Twitter's Civic Integrity Work Around the 2020 Elections

Throughout the 2020 election, we've seen record-levels of election-related conversations on Twitter. Our teams have and will continue to actively work to protect the integrity of this public conversation. We have taken a three-pronged approach to our work around the election, focusing our efforts on protecting our services through our policies, products, and partnerships. We will produce a longer-form retrospective of all of our work around the 2020 US Election in early 2021, but here is an initial post-election assessment.

Policy Updates

In the lead up to the 2020 elections, we made significant enhancements to our policies to protect the integrity of the election. Most notably, this year, we updated our civic integrity policy to more comprehensively enforce labeling or removing of false and misleading information. The updated policy, which we not only announced publicly but also briefed the Presidential campaigns, civil society, and other stakeholders on, covers the following activities:

- * False or misleading information about how to participate in an election or civic process;
- * Content intended to intimidate or dissuade people from participating;
- * Misrepresentation about affiliation (for ex., a candidate or political party);
- * Content that causes confusion about laws and regulations of a civic process, or officials and institutions executing those civic processes;
- * Disputes of claims that could undermine public confidence in the election (e.g. unverified information about election rigging, ballot tampering, vote tallying, or certification of election results); and
- * Content that misleads about outcomes (e.g., claiming victory before results are in, inciting unlawful conduct to prevent the procedural or practical implementation of election results).

The civic integrity policy augmented and enhanced other important rules aimed at preventing interference with the election. Twitter banned all political advertising in 2019, only allowing some cause-based advertising for non-partisan civic engagement,

in line with our belief that the reach of political speech should be earned, not bought. Additionally, we adopted rules prohibiting deceptively shared synthetic or manipulated media, sometimes referred to as ‘deep fakes,’ that may lead to serious offline harm; and labeling deceptive or synthetic media to provide additional context. Moreover, we have rules prohibiting platform manipulation, impersonation, hateful conduct, ban evasion, and attributed activity, among other harmful activities. We have also labeled specific government and state-media accounts from UN P-5 nation states, and plan to expand this effort in the near future.

Providing Context to Limit the Risk of Harmful Misinformation

As we noted in a blog published last week, we applied labels to add context and limit the risk of harmful election misinformation spreading without important context because the public told us they wanted us to take these steps. An initial assessment of our efforts from October 27th to November 11th has found the following:

- * Approximately 300,000 Tweets have been labeled under our Civic Integrity Policy for content that was disputed and potentially misleading. These represent 0.2% of all US election-related Tweets sent during this time period.

- * 456 of those Tweets were also covered by a warning message and had engagement features limited (Tweets could be Quote Tweeted but not Retweeted, replied to, or liked).

- * Approximately 74% of the people who viewed those Tweets saw them after we applied a label or warning message.

- * We saw an estimated 29% decrease in Quote Tweets of these labeled Tweets due in part to a prompt that warned people prior to sharing.

We also got ahead of potentially misleading information by showing everyone on Twitter in the US a series of pre-bunk prompts. These prompts, which were seen 389 million times, appeared in people's home timelines and in Search, and reminded people that the announcement of election results were likely to be delayed, and that voting by mail is safe and legitimate. Our efforts to safeguard the conversation on Twitter about the 2020 US elections continue unabated.

Product Changes

In the weeks leading up to and during election week, we implemented significant product changes intended to increase context and encourage more thoughtful consideration before Tweets are amplified. We are continuing to assess the impact of these product changes to fully understand the effect on the public conversation, which will help guide our work going forward, but I wanted to mention some of our findings today.

We encouraged people to add their own commentary when amplifying content by prompting Quote Tweets instead of Retweets. This change introduced some friction, and gave people an extra moment to consider why and what they were adding to the conversation. The change slowed the spread of misleading information by virtue of an overall reduction in the amount of sharing on the service. We observed a 23% decrease in Retweets and a 26% increase in Quote Tweets, but on a net basis the overall number of Retweets and Quote Tweets combined decreased by 20%.

In addition, we stopped providing ‘liked by’ and ‘followed by’ Tweet recommendations from accounts you don't follow in the Home Timeline and through notifications. While we had initially hoped that this would reduce the potential for misleading information to spread on our service, we did not observe a statistically significant difference in misinformation prevalence as a result of this change (nor any meaningful reduction in abuse reports). Instead, we found that pausing these recommendations prevented many people from discovering new conversations and accounts to follow, and we have since reverted the change.

Partnerships

A core part of our civic integrity efforts included partnerships that allowed us to share information, gather input from experts, and better gain context on how misinformation was being spread and impacting the public conversation. These partnerships included leaders in civic tech, our peers, federal, state, and local governments organizations (e.g., National Association of Secretaries of State, National Association of State Election Directors, Department of Homeland Security, Federal Bureau of Investigation, Department of Justice, Office of the Director of National Intelligence, and elections officials across the country), news organizations, and civil society, among others.

We want to be very clear that we do not see our job in this space as done. Our work here continues and our teams are learning and improving how we address these challenges and earn the trust of the people who use Twitter. I look forward to continuing to work with you on solutions and building the guideposts for the future Internet. Thank you for the opportunity to appear today.

Read this original document at: <https://www.judiciary.senate.gov/download/dorsey-testimony&download=1>

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 138:

House Select Intelligence Committee Holds Hearing on Worldwide Threats

CQ Congressional Transcripts

Mar. 09, 2023 Revised Final

LIST OF PANEL MEMBERS AND WITNESSES

MICHAEL TURNER:

[Begins in progress] Classified or other information protected from public disclosure. It is my privilege to welcome a distinguished panel of leaders to our hearing today to discuss the intelligence community's annual threat assessment. During today's proceedings, we will hear from Lieutenant General Scott Berrier, director of the Defense Intelligence Agency; the honorable William Burns, director of the Central Intelligence Agency; the honorable Avril Haines, director of National Intelligence; General Paul Nakasone, director of the National Security Agency; and the honorable Christopher Wray, director of the Federal Bureau of Investigation.

Thank you all for your service and for your appearance here today. I also want to thank all of our committee members for their cooperation today. We will have both open and closed sessions with our witnesses. Our plan is to complete the open session by noon, adjourn for a lunch break and resume in closed session.

To my opening statement, this is our annual hearing on worldwide threats. It's an opportunity for the intelligence community to come before Congress and the American people to talk about the threats that our nation faces. It also will be an opportunity for us to talk about how we can respond to those threats and what are the needs of the intelligence community.

Our adversaries self-select and today you'll certainly hear about China, Russia, North Korea, Iran and others. We will also be discussing issues about domestic violence extremist groups. Domestic violence extremist groups such as Antifa, have funding, organizational structures, which include communications, training, logistics, illegal activities, especially as we've seen across the country, violence.

Today, when we discussed the intelligence community surveillance of domestic violence extremist organizations, we're certainly going to be discussing the issue of our concerns of the rights of everyday law abiding Americans whose rights may be violated. Since 1977, our committee was formed to respond to abuses by the intelligence community.

We were organized to protect the integrity of our laws, to protect our citizens constitutional rights. Foremost, that is why our committees here. Concurrently, we were also here to protect our national security, to protect our country and its citizens from foreign and domestic adversaries. Now, I want to welcome you to our new intelligence community.

It is new because we have a renewed commitment of both bipartisanship and working on a professional manner. Our committee was opened by an address by the Speaker of the House and by Minority Leader Jeffries where he tasked each and every member of our committee to be dedicated to national security and to working together.

I'm very pleased that Jim Himes and myself, my ranking member, are dedicated to that bipartisan cooperation and to the professionalism. No one is served by members of this committee fighting with each other. We are here to work together. It's what the American people deserve and what the American people expect.

And we will not always agree, but through debate and dialog we will find solutions. One of these issues that will be open for debate is the renewal of 702 of FISA. The Foreign Intelligence Surveillance Act Section 702. 702 is essential. It has provided successes, and it has provided those successes against our adversaries.

However, there have been and there continue to be many abuses of FISA. It must be reformed. Our first step is that we must be honest with the American people. Today, I am going to be looking to each of you for honesty and acknowledgment that FISA has been abused. From that acknowledgment, we can together find solutions and reforms as we work to renew 702 of FISA. To aid in this process, I have appointed a working group, three members of the majority.

Jim Himes will be appointing three members of the minority to the working group. The working group will have equal numbers of Democrats and Republicans. Darren LaHood will be its chair. I've appointed Representative Darren LaHood to chair this working group because of his leadership, expertise and integrity.

Prior to his election to Congress, Darren LaHood served as a career prosecutor at both the state and federal levels. Specifically, he worked for the US Department of Justice as an assistant United States attorney and was selected as the chief terrorism prosecutor in Las Vegas, Nevada. I am confident that his experience in investigating and prosecuting criminal and terrorist activities make him supremely qualified to lead this important bipartisan working group.

I'm excited about the important work this working group is planning to do and under Darren's leadership, I'm confident that they will produce meaningful reform proposals. But I would be remiss if I did not underscore the burdensome task that they have in front of them and the reality that Congress cannot preserve FISA alone.

What we need from each of you is a commitment to work with the committee and Representative LaHood's working group to gain America's trust and to pursue legislative reforms to the FISA process that safeguard and guarantee the constitutional rights of all American citizens. This commitment is necessary because it is the actions of individuals in your organizations who have degraded the public trust and has ultimately put FISA at risk.

It is not Congress that has put FISA at risk. It is your organization. These abuses did not happen somewhere else. They happened underneath the leadership of the individuals that are represented at the table in front of us. That may sound harsh, but the first step in earning back this trust is an ability to admit that there is in fact a problem.

This problem can't be explained as unintentional lying staff mistakes and misunderstandings. It is a problem that will require cooperation with clear and open minds. We cannot undertake a clean reauthorization of 702 without an acknowledgment of the problem. A concerted effort to gain back trust and a commitment to working with Congress toward meaningful reforms.

I know that every member of this committee is committed to pursue the renewal of 702 and understand its importance and the work that it accomplishes for our national security. With that, I yield to my ranking member.

JIM HIMES:

Thank you, Mr. Chairman, and thank you to each of our witnesses for appearing today. We are grateful for the important work that the intelligence community workforce does every day for our nation. The annual worldwide threats open hearing is a unique opportunity for the public to hear directly from intelligence community leadership about the latest assessments of the most pressing national security threats facing the United States.

It's important for the American people to understand the variety of nation states and non-nation state actors that remain serious concern to our intelligence agencies and to the national security of the United States. North Korea's threatening behavior towards the United States and our South Korean allies continues at a high clip, even as their missile program makes rapid progress.

Iran's malign particularly malign and threatening behavior in the region and towards the United States threatens us in the region, our allies in the region, and I fear that Iran's nuclear program has advanced to a point where we would have little warning if they decided to produce weapons grade enriched uranium and move on to the weaponization of that uranium.

Of course, Russia remains a central threat one year into Putin's brutal invasion of Ukraine. Last year, Chairman Turner and I had the opportunity to visit Kyiv and meet President Zelenskyy and his leadership to see firsthand the courage of the Ukrainian people who are defending their homeland. The assistance and support we've provided along with our allies have frustrated Putin's ambitions, but we have clearly a long way to go and some thinking to do about how to make sure that that conflict doesn't continue being the meat grinder that it is. Which brings me to China, which is the central, I believe, strategic challenge we face in the world.

One marked by a complicated and interdependent economic relationship. Last week, we held a hearing with leaders from the foreign policy community and Dr. Richard Haass, most recently of the Council on Foreign Relations, observed that however one might characterize our relationship with China, the easy Cold War analogies to the Soviet Union are inapt.

The Soviet Union was not integrated into the global economy. For all our discussion of decoupling, the United States and China set a new record in 2022 on two way trade between our countries totaling \$700 billion. China currently holds close to \$1 trillion of United States sovereign debt. So how do we respond to an increasingly aggressive and militaristic Chinese approach to world affairs?

China clearly aspires to export its authoritarian approach to governance including the technological tools that enable their regime to restrict speech and surveil their people. How well do we know Chinese thinking, intentions, redline and weaknesses? As the policy makers navigate this difficult path, that will be an essential task for the intelligence community.

A word on technology, which I think I have talked to all of you about. For the first time since the Manhattan Project in the late 1940s, we are not the clear technological leader. Innovation is happening

elsewhere. And of course, innovation is happening at a rapid clip inside China, and we no longer live in the era of planes and tanks and battleships.

Technology today means artificial intelligence, quantum computing and biosynthesis. None of those are areas in which we want to be even a fast follower. We want to be at the point of the spear on innovation on those things. I concur with the chairman on 702. The people sitting here today understand that 702 authorities must be reauthorized.

702, unlike the Section 215 metadata collection program, is a 24/7 day by day essential tool to keeping this country safe. But the chairman's not wrong, the Congress, we have a long way to go to educating the Congress on precisely what those authorities are. I would note that many of the abuses that the chairman made reference to, or misbehavior, occurred not under FISA 702, but under other FISA authorities.

And I note that just because we have a long way to go in educating the Congress of the United States and the people of the United States about exactly what it is that we are talking about. And you have a long way to go to validating my statement that this is a 24/7 day by day essential tool to keeping the American people safe.

So I look forward to our conversation, concur in the chairman's view that we are committed to pursuing the important work of this committee in a bipartisan thoughtful and constructive way, and welcome you again to testimony here today.

MICHAEL TURNER:

Thank you, Congressman Himes. We now turn to Avril Haines, director of national intelligence who will be presenting the opening statement on behalf of the panel. Welcome and thank you for your leadership, Director Haines.

AVRIL HAINES:

Thank you very much. Chairman Turner, Ranking Member Himes, members of the committee, thank you for the opportunity to be here today alongside my wonderful colleagues and on behalf of the extraordinary public servants we lead in the intelligence community, to present the IC's annual threat assessment. And before I start, I just want to publicly thank the men and women of the intelligence community whose work we're presenting today.

From the collector to the analyst and everybody in between who made it possible for us to bring you the annual threat assessment in hopes that this work will help keep our country safe and prosperous, thank you. This year's assessment notes that during the coming year, the United States and its allies will face an international security environment that is dominated by two sets of strategic challenges that intersect with each other and existing trends to intensify their national security implications.

First, great powers, rising regional powers and an evolving array of non-state actors are vying for influence and impact in the international system, including over the standards and rules that will shape the global order for decades to come. The next few years are critical as strategic competition with China and Russia intensifies and in particular, over how the world will evolve and whether the rise of authoritarianism can be checked and reversed.

How well we stay ahead of and manage this competition will be fundamental to our success in navigating everything else. Second, challenges that transcend borders, including climate change, human and health security and economic needs made worse by energy and food security as well as Russia's unprovoked and illegal invasion of Ukraine are converging as the planet emerges from the COVID-19 pandemic, and all at the same time as great powers are challenging longstanding norms for transnational cooperation.

Further compounding this dynamic is the impact that rapidly emerging Technologies, Ranking member Himes, noted are having on governance, business, society and intelligence around the world. And given that background, the People's Republic of China, which is increasingly challenging the United States economically, technologically, politically and militarily around the world, remains our unparalleled priority.

Chinese Communist Party or CCP under President Xi Jinping will continue efforts to achieve Xi's vision of making China the preeminent power in East Asia and a major power on the world stage. The CCP is increasingly convinced that it can only fulfill Xi's vision at the expense of US power and influence and by using coordinated whole of government tools to demonstrate strength and compel neighbors to acquiesce to its preferences, including its land, sea and air claims in the region and its assertions of sovereignty over Taiwan.

Last October, President Xi secured his third five year term as China's leader of the 20th party Congress. And as we meet today, China's national legislature is in session, formally appointing Xi and confirming his choice to lead the PRC's State Council as well as its ministries and the Leaders of the military, legislative and judicial branches.

AVRIL HAINES:

And after more than a decade serving as China's top leader, Xi's control over key levers of power give him significant influence over most issues. Xi has surrounded himself with like-minded loyalists at the apex of the party's standing committee, China's highest decision making body. And we assess that during the course of Xi's third term, they will together attempt to press Taiwan on unification, undercut US influence which they perceive as a threat, drive wedges between Washington and its allies and partners, and promote certain norms that favor China's authoritarian system. You may have seen Xi's recent criticism during his speech on Monday of what he referred to as America's suppression of China, reflecting his longstanding distrust of US goals and his apparent belief that the United States seeks to contain China.

Xi's speech was the most public and direct criticism that we have seen from him to date, and probably reflects growing pessimism in Beijing about China's relationship with the United States, as well as Xi's growing worries about the trajectory of China's economic development and indigenous technology innovation, challenges that he now blames on the United States.

He also wants to message his populace and regional actors that the US bears responsibility for any coming increase in tensions. Despite public and directly critical rhetoric, however, we assess that Beijing still believes it benefits most by preventing a spiraling of tensions and by preserving stability in its relationship with the United States.

Specifically, Beijing wants to preserve stability in East Asia, avoid triggering additional economic punishments from US sanctions and US partners, and showcase a steady relationship with the United States to avoid setbacks in its other relationships around the world, even while signaling opposition to claimed US provocations, including the shoot down of the PRC balloon.

He wants a period of relative calm to give China the time and stability it needs to address domestic difficulties. Xi's principal focus is on domestic economic development, which is not assured. The IC assesses that China's long term economic growth will continue to decelerate because China's era of rapid catch up growth is ending, and structural issues such as debt, demographics, inequality, overreliance on investment, and suppressed consumption remain.

And although the CCP may find ways to overcome its structural challenges over the long term, in the short term the CCP continues to take an increasingly aggressive approach to external affairs, pursuing the goal of building a world class military, expanding its nuclear arsenal, pursuing counter space weapons capable of targeting US and allied satellites, forcing foreign companies and coercing foreign countries to allow the transfer of technology and intellectual property in order to boost its indigenous capabilities, continuing to increase global supply chain dependencies on China with the aim of using such dependencies to threaten and cut off foreign countries during a crisis, expanding its cyber pursuits, and increasing the threat of aggressive cyber operations against the US homeland and foreign partners, and expanding influence operations, including through the export of digital repression technologies.

The CCP will also seek to reshape global governance in line with his preferences and governance standards that support its monopoly of power within China. Beijing is elevating PRC candidates and policies at the UN, attempting to gain buy in for Xi's development and global initiatives, promote blocs like the Shanghai Cooperation Organization as a counterweight to the West, and shape multilateral groupings such as the formerly 17+1 forum in Eastern Europe, but with mixed success.

In brief, the CCP represents both the leading and most consequential threat to US national security and leadership globally, and its intelligence specific ambitions and capability make it our most serious and consequential intelligence rival. During the past year, the threat has been additionally complicated by a deepening collaboration with Russia, which also remains an area of intense focus for the intelligence community.

And when we were here last before the committee for the ATA annual threat assessment last year, it was only a few weeks after Russia's unprovoked and illegal invasion of Ukraine. Now we're over a year into the war, which is reshaping not only Russia's global relationships and strategic standing, but also our own, strengthening our alliances and partnerships in ways that President Putin almost certainly did not anticipate, often precipitating the very events that he hoped to avoid, such as Sweden and Finland's petition to join NATO. And on the battlefield, there is currently a grinding attritional war in which neither side has definitive military advantage and the day to day fighting is over hundreds of meters, currently focused in Donetsk as Russia tries to capture the remainder of the oblast.

The Russians are making incremental progress on Bakhmut, which is not a particularly strategic objective, but the otherwise -- but are otherwise facing considerable constraints, including personnel and ammunition shortages, dysfunction within the military's leadership, exhaustion, and morale challenges. And even as the Russian offensive continues, they are experiencing high casualty rates.

Putin is likely better understanding the limits of what his military is capable of achieving, and appears to be focused on more modest military objectives for now. Export controls and sanctions are hampering Russia's war effort, particularly by restricting access to foreign components necessary to produce weapon systems.

And if Russia does not initiate a mobilization, a mandatory one, and identify substantial third party ammunition supplies, it will be increasingly challenging for them to sustain even the current level of offensive operations in the coming months, and consequently they may fully shift to holding and defending the territories they occupy.

In short, we do not foresee the Russian military recovering enough this year to make major territorial gains, but Putin most likely calculates that time is on his side, and prolonging the war, including with potential pauses in the fighting, may be his best remaining pathway to eventually securing Russia's strategic interests in Ukraine, even if it takes several years.

And Ukraine, of course, also faces challenges. Ukraine's prospects for success in a major spring offensive will probably hinge on several factors. At present, the Ukrainian armed forces remain locked in a struggle to defend against Russian offenses across eastern Ukraine. And while these Russian assaults are costly for Russia, the extent to which Ukrainian forces are having to draw down their reserves and equipment as well as suffer further casualties will all likely factor into Ukraine's ability to go on the offensive later this spring.

The IC continues to monitor Putin's reactions and his nuclear saber rattling. Our analysts assess that his current posturing is intended to deter the West from providing additional support to Ukraine as he weighs a further escalation of the conflict. And he probably still remains confident that Russia can eventually militarily defeat Ukraine, and wants to prevent Western support from tipping the balance and forcing a conflict with NATO. And of course, the already considerable human toll of the conflict is only increasing.

In addition to the many tens of thousands of casualties suffered by the Russians and Ukrainian militaries, more than eight million people have been forced to flee Ukraine since Russia invaded. There is widespread reporting of atrocities committed by Russian forces, including deliberate strikes against nonmilitary targets, such as Ukraine civilian population and civilian infrastructure, particularly its energy facilities and electrical grid.

Russia and its proxy groups almost certainly are using so-called filtration operations to detain and forcibly deport tens of thousands of Ukrainian civilians to Russia. And the IC is engaged with other parts of the US government to document and hold Russia and Russian actors accountable for their actions.

The reaction to the invasion from countries around the world has been resolute, hurting Russia's reputation in the world and generating criticism at home. Moscow has suffered losses that will require years of rebuilding, and leave it less capable of posing a conventional military threat to Europe and operating assertively in Eurasia and on the global stage.

And as a result, Russia will become even more reliant on asymmetric options such as nuclear, cyber, and space capabilities, and on China. Our assessment also covers Iran, which continues to pursue its longstanding ambitions for regional leadership and is a threat to US persons directly and via proxy attacks.

Iran also remains a threat to Israel, both directly and indirectly, through its support of Lebanese Hezbollah and other proxies. And most concerning, Iran has accelerated the expansion of its nuclear program, stating that it is no longer constrained by any JCPOA limits and has undertaken research and development activities that would bring it closer to producing the fissile material for completing a nuclear device following a decision to do so. North Korea similarly remains a proliferation concern as it continues its efforts to steadily expand and enhance its nuclear and conventional capabilities targeting the United States and our allies, periodically using aggressive and potentially destabilizing actions to reshape the regional stability environment in its favor and to reinforce its status as a de facto nuclear power.

In addition, regional challenges such as inter-state conflicts, instability, and poor governance developments also pose growing challenges in Africa and the developing world. Increased poverty, hindered economic growth, and widespread inequality are creating the conditions that are feeding domestic unrest, insurgencies, democratic backsliding, authoritarianism, and cross border conflict spillover.

And several parts of the Middle East will remain plagued by war, insurgencies, and corruption. In the Western Hemisphere, persisting economic weakness, insecurity, corruption are fueling public frustration, and anti-status quo pressures very likely will present governance challenges to leaders, while also posing sustained spillover migration, criminal, and economic challenges for the United States.

Throughout the world, countries are struggling to maintain democratic systems and prevent the rise of authoritarians, in some cases because Russia and China are helping autocrats take or hold power. And as I noted at the outset, transnational challenges interact with more traditional threats and often reinforce each other, creating compounding and cascading risks to US national security.

For example, climate change remains an urgent threat that will increasingly exacerbate risks to US national security as the physical impacts increase and geopolitical tensions mount over the global response to the challenge. And now entering the fourth year of the COVID-19 pandemic remains one of the most significant threats, excuse me, to global public health, at a cost of more than 6.5 million and trillions of dollars in lost economic output to date.

In addition to direct effects of the pandemic, resultant economic, human security, political, and national security implications of COVID-19 continue to strain recovery efforts, presenting both known and unforeseen challenges that probably will ripple through society and the global economy during the next year and for years to come.

Russia's aggression against Ukraine has aggravated COVID-19 related fragilities in the global economy, raised commodity prices, fueled market volatility, and contributed to food insecurity and financial instability. And the combination of elevated energy and food prices has increased the number of individuals facing extreme poverty and food insecurity.

Affected countries will struggle to reverse these trends through 2023, even if global food prices stabilize. And Russia's war in Ukraine can be blamed for these intensifying effects, something much of the world also understands and that others, including China, will have to come to terms with as they consider to what extent they want to continue assisting or enabling Russia.

And climate change, the pandemic, and conflicts are exacerbating irregular migration. And in the Western Hemisphere, push and pull factors that drive migrants to the United States, such as deteriorating socioeconomic and security conditions, misperceptions of US policies and employment opportunities in the United States, will almost certainly persist through 2023. And please forgive me, because apparently the last two pages of my -- did not print out on this, so I'm just going to grab my extra copy.

Oh, for heavens sakes. Transnational criminal organizations exploit migrants through extortion, kidnapping, and human trafficking, including sex trafficking and forced labor. And these organizations also continue to pose a direct threat through the production and trafficking of lethal illicit drugs, massive theft, financial and cyber crimes, money laundering, and eroding the rule of law in partner nations.

In particular, the threat from illicit drugs is at historic levels, with the robust supply of synthetic opioids from Mexican TCOs continuing to play a role in driving American overdose to over 100,000 annually. And terrorism, of course, remains a persistent threat, but the problem is evolving. Individuals and cells adhering to ideologies espoused -- espoused by ISIS, al-Qaida, and transnational racially and ethnically motivated violent extremist movements in particular pose significant threats to US persons, facilities, and interests.

And then two indirect threats that I think are worth highlighting. New technologies, particularly in the fields of artificial intelligence and biotechnology, are being developed and proliferating faster than companies and governments are able to shape norms governing their use, protect privacy challenges associated with them, and prevent dangerous outcomes that they can trigger.

The convergence of emerging technologies is likely to create breakthroughs that are not as predictable and that risk a rapid development of more interconnected asymmetric threats to US interests. Relatedly, foreign states' malicious use of digital information and communication technologies will become more pervasive, automated, targeted, and complex during the next few years, threatening to distort publicly available information and probably outpacing efforts to protect digital freedoms and at the same time educate audiences on how to distinguish fact from propaganda.

Authoritarian governments usually are the principal offenders of digital repression. And of course, democracies with open information environments are the most vulnerable. In closing, I want to bring to your attention the absolutely crucial authority that both Chairman Turner and Ranking Member Himes discussed will expire at the end of the year if Congress does not act, which is 702 of the Foreign Intelligence Surveillance Act. I can tell you without hesitation that Section 702 was relied upon in gathering intelligence that was relevant to putting together this assessment, as it is hard to overestimate the importance of this authority to our work every day.

AVRIL HAINES:

FISA Section 702 provides unique intelligence on foreign intelligence targets at a speed and reliability that we cannot replicate in any other authority. Section 702 was originally enacted to enable the US government to quickly collect on the communications of terrorists located abroad. The authority allows the IC to acquire foreign intelligence from non-US people located outside of the United States who are using US electronic communication service providers, 702 is still vital to our counterterrorism mission as

evidenced by its key role in the US government's operation against former al-Qaida leader, Ayman Al-Zawahiri.

But 702 is now principally relied upon for vital insights across a range of high priority threats, including China, malicious cyber actors targeting US critical infrastructure, weapons proliferation, attempting to evade sanctions to deliver precursor chemicals to hostile actors and even key intelligence related to threats emanating from Russia, North Korea, Iran.

And I'll say China, again. I realized that Section 702 is a powerful authority and it's incumbent on all of us in the intelligence community to ensure that the privacy and civil liberties interests of Americans are built into its design and implementation at every level. Over the last many years we have significantly expanded oversight and dedicated resources to compliance in order to do just that.

And we welcome the opportunity to work with you on reauthorizing this critical authority and building in your trust. Thank you for your patience and we'll look forward to your questions. Thank you.

MICHAEL TURNER:

Well, Director Haines, it was incredibly impressive to watch you to continue to read your statement while looking through your file. I don't know that any of us would have been able to do that. But Director Burns for the win. That was great.

AVRIL HAINES:

As always.

MICHAEL TURNER:

Excellent. We'll now begin with member questions, and I yield my time to Representative Darin LaHood, the chair of our FISA 702 Working Group. Darin?

DARIN LAHOOD:

Well, thank you, Chairman Turner. And I want to thank the panel here today for your service to our country and thank you for the work you do every day to keep our citizens safe and our country secure. I'm honored to be selected as the lead for this important working group on FISA reforms and I'm excited to take on the necessary review.

I concur with Chairman Turner that FISA and specifically the authorities in Section 702 provide our intelligence community with an invaluable and irreplaceable tool that supports our national security apparatus in the fight against our foreign adversaries. As a former assistant US attorney and specifically as a chief terrorism prosecutor overseeing the investigation and criminal prosecution -- prosecutions of terrorist activities, I fully understand the value of FISA as an incredible collection asset in our fight against ongoing global and terrorist threats.

This committee has been briefed countless times on the many successes directly attributable to our 702 collection authorities, some of which, Director Haines, you highlighted in your opening remarks. And I would also comment, I know General Nakasone last month or I guess in January you spoke to the Privacy

and Civil Liberties Oversight Board on the value of 702. In that speech, you talked about this authority provides the US government with irreplaceable insights.

Whether we are reporting on cyber security threats, counterterrorism threats, or protecting US and allied forces, FISA Section 702 has helped us understand the strategic intention of the foreign governments we are most interested in, including the PRC, Russia, Iran, and North Korea. Unfortunately, there are far too many members of Congress on both sides of the aisle that question whether the executive branch can be trusted with this powerful tool and that's because of their -- in the past and currently, there has been abuses and misuses of 702 by the FBI. From where I sit today, I believe that a clean legislative reauthorization of 702 is a nonstarter.

To reiterate what the chairman said, you must first acknowledge that a problem exists before we can formulate meaningful reforms to build back trust and confidence in the FISA process. Director Wray, I want to start with you and ask, are you willing to acknowledge that the FBI has committed abuses and violations in its use of FISA? And is that defensible?

CHRISTOPHER WRAY:

Well, first off, no violations are defensible in my view. It's important to distinguish as I think both the ranking member and the chair may have between things that happen with Title one FISA, you know, for example that were at issue in the inspector general report related to the Crossfire Hurricane matter, which as I've said before, describes conduct that I consider totally unacceptable, totally unacceptable, and unrepresentative of the FBI. And we implemented all sorts of reforms that I could go into on that.

Then over on the 702 side, there have been compliance incidents that have to be addressed. And we have taken all sorts of steps that I could walk the committee through here to address that issue. And what's important to note about that is that all of the reports to date that have been shared with the public and I think with the Congress about 702 compliance issues all predate.

That is the conduct at issue predate all these reforms, which is why it's so important for me to be able to let the committee know and this will be coming in the -- in more detail in the next ODNI report that comes out in late April, I think it is, that we have now seen a 93 percent decrease year over year from '21 to '22 in the number of US person queries made by the FBI. And that's not just an aberration of that one year.

If you compare it to 2020, so the year before that, it's about an 85 percent increase. So it's a dramatic increase in the judiciousness with which our people are running their queries. And we are absolutely committed to making sure that we show you, the rest of the members of Congress, and the American people that we're worthy of these incredibly valuable authorities.

DARIN LAHOOD:

Well, I appreciate you mentioned that. I would say because of a number of these abuses and non-compliance issues with the FBI, would you agree that the FBI has a trust issue with the American public and specifically with members of Congress?

CHRISTOPHER WRAY:

Well, certainly any time we have anybody who has a trust issue with us, we want to try to address it. I think what I see -- look at the American people more broadly, I think a lot of it is reaction to specific cases and things here and there. But I will tell you that I see the American people showing up in droves to come work at the FBI. That -- putting that to the side -- putting that to the side, we clearly have work to do and we're eager to do it with this committee to show that we can be worthy stewards of these important authorities.

And so, if there are questions that are -- that need to be answered, I understand completely why those questions are being raised. We brought them on ourselves. And I want to make sure that we can show you that we can answer those questions.

DARIN LAHOOD:

And how do you give reassurance to the American people that their civil liberties are going to be protected?

CHRISTOPHER WRAY:

Well, the changes that I started describing at a high level include all sorts of things. So that's everything from system changes that prevent even inadvertent compliance incidents. That's new safeguards, new approvals, new oversight, all sorts of mandatory enhanced training. I created and stood up an entire new Office of Internal Audit that did not exist at the FBI before and brought in a former agent who's also a former big four accounting firm partner to run that Office of Internal Audit.

And that office is focused exclusively on FISA compliance. Ultimately, in the long run, we want that office to take on other kinds of compliance, too. But because of the importance of this issue, because of the importance of the concerns that you and others have framed, we've dedicated that Office of Internal Audit to focus exclusively on this important authority and compliance with it. So those are some of the things.

Obviously, there's a lot more that I could get into, but I'm sympathetic to the time constraints here.

DARIN LAHOOD:

Well, thank you for that. Unfortunately, I believe that the FBI does have a significant trust issue with members of Congress and that's part of what we'll deal with with the working group. And it's -- I would say that trust has only been made worse by the recently declassified Section 702 compliance report covering December 2019 through May of 2020. In that report, there was a number of concerning things that were brought forward.

There was queries done inappropriately by the FBI on a local political party. And then secondarily, included in there was one specific instance of abuse involving multiple queries of a sitting member of Congress in the FBI's FISA databases. Buried in a footnote of the declassified assessment, this specific incident described as follows, quote, an intelligence analyst with the FBI conducted multiple queries using only the name of a US Congressman.

The 707 report describes the specific facts that led the analyst to conduct these queries. These queries retrieved unminimized FISA acquired information including Section 702 acquired products that were

opened. FBI advised that no minimized FISA acquired information was disseminated or used in any way. This was reviewed obviously by the National Security Division of the US Department of Justice and ODNI. And based on what they reviewed, they found these queries to be wholly inappropriate, not compliant, and a violation because they were overly broad as constructed.

I think that the report's characterization of this FBI analyst action as a mere misunderstanding of querying procedures is indicative of the culture that the FBI has come to expect and even tolerate. It is also indicative of the FBI's continued failure to appreciate how the misuse of this authority is seen on Capitol Hill.

And I want to make clear the FBI's inappropriate querying of a duly elected member of Congress is egregious and a violation not only that degrades the trust in FISA but is viewed as a threat to the separation of powers. I have had the opportunity to review the classified summary of this violation and it is my opinion that the member of Congress that was wrongfully queried multiple times solely by his name was in fact me. Now, this careless abuse of this critical tool by the FBI is unfortunate.

Ironically, I think it gives me a good opportunity and a unique perspective on what's wrong with the FBI and the problems that the FBI has. To highlight that, I would like to submit for the record a couple of things. February 28th, 2023, Director Haines and Attorney General Garland asked for a reauthorization from the Congress.

But they go in to add that there needs to be rigorous and ongoing oversight of the FBI's 702 querying. Specifically, their collection decisions on US person inquiries and they will be evaluating and taking remedial action to address identified incidents of noncompliance by the FBI. I'd like to submit that for the record, Mr. Chairman.

MICHAEL TURNER:
Without objection.

DARIN LAHOOD:

Secondly, a letter was sent to you on February 15th, Director Wray, 2023 from Congressman Andy Biggs of Arizona, and he talks about the declassified 2021 report detailing these continued abuses of 702. In there, he mentions that these instances should frighten every American and Congress deserves an explanation for them.

He additionally talks about these, quote, back door searches are a violation of the Fourth Amendment and cannot continue. I'd ask to submit that for the record.

MICHAEL TURNER:
That objection.

DARIN LAHOOD:

Thirdly, article in Politico from March 1st titled DOJ Faces Bipartisan Phalanx or Army of Skeptics on FISA 702. In that article, again referring to this declassified report on the inappropriate use of 702, it talks

about in a sign of -- I'll quote here -- and a sign of odd political bedfellows in the House who are pushing reforms.

Conservative Congressman Andy Biggs and progressive member Pramila Jayapal, both members of the Judiciary Committee, publicly vetted on the detail tucked in the footnote of the report, an FBI intelligence analyst improperly queried surveillance data on a US member of the House. I'd asked to submit that for the record.

MICHAEL TURNER:
Without objection.

DARIN LAHOOD:
Lastly, the footnote that I mentioned that has been declassified states in there that the National Security division of the US Department of Justice and ODNI assessed based on the facts and analysis of this FBI analyst that these queries were not compliant because they were overly broad as constructed. I'd like to submit that for the record.

MICHAEL TURNER:
Without objection.

DARIN LAHOOD:
The bottom line is 702 deserves to be reauthorized because it's an invaluable tool to our efforts to counter the threats of our adversaries. But the FISA working group must and will pursue reforms and safeguards through this reauthorization process. To help explain to the public why 702 should be reauthorized, I have a few questions for other panelists.

Director Haines, why do we need 702 to specifically counter China?

AVRIL HAINES:
Thank you, representative. Specifically with respect to China, there are a number of ways in which 702 is crucial. It's crucial in the context of counterintelligence where we are looking at where it is that China's efforts to send spies into the United States may be and what their planning is in relation to it. It is crucial in the context of threats to our, you know, to US victims and to critical infrastructure through cyber.

As we've all indicated, it's crucial to understanding a whole range of issues because it is effectively the most effective way for us to gather intelligence against non-US persons outside of the United States.

DARIN LAHOOD:
Thank you. And Director Burns, what does 702 mean for the CIA's ability to counter China?

WILLIAM BURNS:

It's crucially important for all the reasons, sir, that Director Haines just mentioned. It also enables us to focus on efforts to evade sanctions, to steal intellectual property, to obtain sensitive technologies as well. And so in all those areas is extremely important.

DARIN LAHOOD:

And Director Nakasone, can you quantify in some way how vital 702 is to the NSA's efforts to counter China? And I know you specifically referenced a number of incidents -- that in your speech in January.

PAUL NAKASONE:

I would quantify it, congressman, by saying it is the number one authority that we need. I can go into close session with regards to the specific areas where it is so important.

DARIN LAHOOD:

Thank you. And Director Berrier, as a consumer of the information obtained by 702, can you explain the value of this information in DNI's efforts to counter China?

SCOTT BERRIER:

Yes, I can. As an all source intelligence agency, while we don't do FISA collection, we certainly benefit from the insights we get from that. We bake that into our all source analysis to eliminate threats for the Department of Defense and the nation.

DARIN LAHOOD:

Thank you for that. In closing, I'm honored by Chairman Turner's selection as the chair of the FISA working group. And I'm energized to begin our bipartisan work with the Judiciary Committee and our Senate colleagues to reform and reauthorize this vital tool. I also look forward to working with all of you here before us today and request your cooperation in this endeavor.

Thank you. And I yield back, Mr. Chairman.

MICHAEL TURNER:

Thank you. Member Himes.

JIM HIMES:

Thank you, Mr. Chairman. And thank you again to our witnesses. My good friend from Illinois put a lot of on the table there, much of which unfortunately I was not briefed on. So, Director Wray, I'd love to start just by giving you a minute or two to respond, if you would like, but I'd like you to keep it to a minute or two if you would.

CHRISTOPHER WRAY:

Obviously, there's a lot to say, so I'll be very brief. I completely understand Congressman LaHood's concerns and everything he read. The main point I would make for today's purposes is that all of those problems, and they are problems, all of those compliance violations, and they are violations predate, predate all of these reforms that I was trying to summarize.

And so my hope is that we will be able to show by working with the working group how these reforms will prevent stuff like what you described from happening again in the future.

JIM HIMES:

Thank you, Director Wray. I'm going to direct my next question to Director Haines and Director Burns. We spent a lot of time thinking about the mechanics and tactics of what conflict with China would look like. And we don't spend a lot of time thinking about the economics of tension leading to ultimately conflict where that to occur.

This is not current but RAN did a study in which they estimated that Chinese GDP in the event of a conflict would contract by a staggering 25 to 35 percent. US GDP could contract by 5 to 10 percent if there was conflict in the Taiwan Strait. So the perplexing thing here is this is a country that really the sole reason that it has been able to achieve the economic growth that it has to the point where today it's on an aggregate basis, the largest economy in the world, has been engagement with the world.

Licit engagement through trade and other things and illicit engagement through the stealing of IP, the manipulation of currency rates over time, et cetera. So, I wonder -- two-part question. Can you paint a picture of if we continue to -- if tensions continue to be exacerbated leading to a point where there is conflict, what that would look like for the global economy for the Chinese economy?

And most importantly, help me understand why a Chinese leader would risk the golden goose essentially?

AVRIL HAINES:

I'll start. So I think to your point, representative, I -- it is not our assessment that China wants to go to war. And that is something I think to start with. In other words, they are, you know -- we continue to assess that, for example, even with respect to Taiwan that they would prefer to achieve unification through peaceful means as opposed to through a use of force.

They nevertheless are utterly committed to unification, and I think that is the challenge. In other words, she has made it quite clear that that is something that has to happen. And as a consequence, if they believe that peaceful unification is not an option, then they are in the potential for actually trying to achieve it militarily.

And they are certainly planning for that potential. And then in terms of the impact that it would have, I think, you know, obviously it depends on what the conflict looks like. But to your point, again, I think it's absolutely right that this is -- any conflict is likely to have enormous economic implications.

And one of the things that we have certainly looked at and that others, you know, within the government, Treasury and Commerce, and so on, have looked at is the implications with respect to Taiwan of a disruption of their materials, particularly their semiconductors. And we've, you know --

studies show that it would actually have an absolutely enormous implications for the global financial economy if there were disruption to Taiwan semiconductor production because really, you know, Taiwan -- the semiconductors, the chips that come out of Taiwan are present in virtually every category of electronic devices around the world.

Leave it at that.

JIM HIMES:

Director, I know CIA conducts economic work and economic assessment. So I'd be interested in your view.

WILLIAM BURNS:

Sure. And just -- and I would just add two examples to what Director Haines said in terms of the calculus of the Chinese leadership both on Taiwan and in terms of its relationship with Russia. I think on Taiwan, well as Director Haines said, we don't see evidence today that she has made a decision to invade Taiwan.

It's -- I would never underestimate the ambitions of the current Chinese leadership in that regard or their determination. I do think that nobody has watched more intently Vladimir Putin's experience in Ukraine than Xi Jinping has. And I think he's been sobered to some extent at least it's our analysis by the extent to which the West was able to maintain solidarity and absorb some short-term economic costs in the interest of imposing even greater long term economic costs on Russia.

That's something that President Xi has to weigh as he comes out of Zero-COVID, tries to restore Chinese economic growth, tries to engage with the rest of the global economy. And I think that also weighs in his decision about whether or not to supply lethal equipment to Russia. We see clear evidence that the Chinese leadership is considering that.

Not that it's made a decision, not that it's begun lethal shipments. But there again I think that economic factor, as Director Haines said, has to weigh significantly in the calculus of the Chinese leadership.

JIM HIMES:

Do we believe that the Chinese leadership sufficiently appreciates even where they supply lethal weapons that would have economic consequences? An awful lot of people around the world would be much more hesitant to do business with China. Do we believe that the leadership in Beijing understands how that is a first step towards again killing the golden goose that has allowed that country to grow economically?

WILLIAM BURNS:

I think the only -- the only thing that I would highlight, congressman, is that I think it's been important that European leaders have spoken up on this issue as well because I think for a long time, the Chinese leadership has assumed that it could drive wedges between the United States and our European allies on an issue like this.

I think the fact that several prominent European leaders have spoken out directly about this is a very important step.

JIM HIMES:

Thank you. Second category of questions is on technology, and I want to be respectful of my colleague's time. So I'm going to direct the questions to General Nakasone and General Berrier. I had the opportunity last week to visit CIA and see the work that's been doing -- been done by the director in terms of technological innovation.

Director Burns has made it a strategic priority. He hired somebody from the outside to be chief technology officer. The visit was amazing. This new chief technology officer cleared out offices, created an open floor space. There's free snack. It's -- they're just missing a millennial playing the guitar to reproduce what you see in Palo Alto every day in the middle of CIA headquarters.

So with that as context, what are you guys doing? I'll start with you, General Nakasone. What are you guys doing that is as tangible as what CIA has done to make sure that we are at the cutting edge of technological innovation?

PAUL NAKASONE:

One of the things we've done, ranking member, is look at different partners. This is the key piece of what we've learned from Russia, Ukraine. The private sector has been incredibly helpful in terms of where we need to go in being able to thwart what Russia has attempted to do in Ukraine. We've opened up a cyber space collaboration center, an unclassified building where our analysts go to engage with the private sector and members of the defense industrial base to do two things.

One is to provide information in the defense industrial base in terms of what is going on in the domain of cyber space. Two is to also get information from what we're seeing out there. What are the new leads? What are the things that we have to be able to emphasize? The coming decade is certainly a decade where cyberspace will be dominated.

JIM HIMES:

One of the things that we believe is that we have to have those partnerships that are so critical. General Berrier.

SCOTT BERRIER:

Congressman, our innovation engine is really fueled by this thing called NeedipeDIA. This is where -- NeedipeDIA where companies can come in with great ideas on how they might be able to help the Defense Intelligence enterprise. We evaluate those ideas. We meet with those folks. And then we try to pull their ideas in. Our two major focus areas right now are AI and ML for our program called MAARRS, the Machine Assisted Analytic Rapid Repository System which will revolutionize the way we do foundational military intelligence.

Really pulling in swaths of data to make that environment much richer for our analysts. And the other piece is really our MASINT sensor modernization to be able to take all of those varieties of signals that

are out there that are new and unique and be able to pull them into our MASINT enterprise. That's the focus.

JIM HIMES:

Thank you. General Berrier, I appreciate that. And I'm glad you highlighted openness to outside companies that are not the traditional primes. I think that only gets you about a third of the way there because I've just heard too many stories of innovative companies who just have no hope of navigating the acquisition process and authorities and everything else.

Even though they may have cutting-edge technology far better than what would be. So I'm going to follow up with you on that and yield back my time. Thank you, Mr. Chairman.

MICHAEL TURNER:

Thank you. Dr. Wenstrup.

BRAD WENSTRUP:

Well, thank you, Chairman Turner, Ranking Member Himes, and all of you for being here today. Director Haines, you cut right to it today about the challenges that we face as a nation. The threats that we have. Threats to our country are not new, but some of the forms of those threats are new. And I want to talk about that a little bit.

The Chinese Communist Party is very assertive. They want to destabilize us as much as they can and they're getting pretty good at it. So growing concerns I have are the development of adversaries' biological weapons is of great concern to me and also the flow of illicit fentanyl coming into our country, which even in a meeting with the Chinese ambassador, he admitted we sell the precursors.

Those are legal products. You know, it's somebody else's problem after that. Well, it is our problem. And I do want to hold those accountable for these efforts to be held accountable at some point And we've got to do a better job of that. And I think we need to address and invest in the resources we need to stop the scourge of this fentanyl -- illicit fentanyl.

And also the creation of bioweapons is something we should be greatly concerned about, as with any weapon an adversary may carry. So it's our responsibility, I think, to really work together on these things as best we can. We had a panel a few weeks ago, Doctor Heather Wilson was there, and I asked how we could work together a little bit better in her eyes.

And she mentioned how the law requires members of this committee to be kept fully and currently informed of the intelligence activities of the United States. That's this committee. It's not every member of Congress. It's not the general public. And we all get that. But for this committee, it has to happen, and we need to insist upon that.

And we also need to insist on our side that we engender trust to the seriousness of this committee and the work that we have to do and our own professional responsibilities in this relationship. And I think we're at that point, I really do, with this committee right now. But we have the responsibility of oversight as well as working with all of you.

And in my mind, there can be no walls between us. There can be walls around us at times. There needs to be walls around us at times, but there should be no walls between us if we're going to be effective. And we really can only move at the speed of trust. And I feel like I've developed relationships with all of you.

It's been very helpful to the work that we do on this committee, and I thank you for that. Sometimes we can do a little bit more. And so Director Haines, I know this committee has written you a few times about who the intelligence community consulted with regarding the assessment of COVID-19 and its origins.

Now I chair the Select Subcommittee on the Pandemic, all things with the pandemic and origins of COVID is important. And even yesterday in our hearing, every person on the committee, bipartisan, and every one of our panelists said finding the origins of COVID is an important project we need to continue and try to get to. And we can go into all those reasons.

You know, why is it important, though, that -- for us to have this information and to know who the experts are? And you know, if we hear something like it's our policy not to tell you on the committee who we spoke to, that's a problem. And it is important who you spoke to because if who someone spoke to may have some personal bias or other agenda or political bias towards their conclusions, I mean, look, you see -- you've seen all these agencies with different conclusions.

Well, why is that? Well, part of that may be depending upon who they talk to. So that is important that we get that information. And it's my understanding that the DOE would be willing to show us their underlying report, especially their updated report. But since ODNI owns the assessment, you'd have to approve that.

So what I'm going to ask is that you would approve that and get us that information so that we can move forward. And I would hope that we can also get the information of actually who they talk to. It's important to this committee. It's important to the country. So I guess I'm just asking, would you commit to that at this time?

AVRIL HAINES:

Thank you so much, congressman. I know this is an issue that we've talked about before. And I think -- first of all, on the DOE assessment, absolutely. I suspect it would have to be in classified form. I'm sure it's a classified report. But more than happy to share any final assessment that they've done if they're comfortable with it. I can't imagine myself standing in the way.

AVRIL HAINES:

So I don't know what that is, but we'll look into that and get back to you quickly. I think on the more general issue, let me just put a few things down. I think one problem for us is that we obviously want to be able to consult with outside expertise including academics, variety of other experts in fields related to COVID-19, but also a series of other areas that we work in. And often for many academics that we consult with, it's not something they want to -- they do not want to be known as consulting with the intelligence community.

It creates challenges for them. And --

BRAD WENSTRUP:

If I may, I'm talking about in a classified setting.

AVRIL HAINES:

No, no, no. So let me finish.

BRAD WENSTRUP:

And this is important to the work because we do need to know who they are and how they came to their assessment.

AVRIL HAINES:

Congressman, let me just finish. I'll explain.

BRAD WENSTRUP:

Sure.

AVRIL HAINES:

So often what will happen is they will, for example, be willing to participate in a conference or something along those lines that's not for us, and they will do it under Chatham House rules that says that we can't attribute, essentially, anything to them specifically even though we can bring the information out.

That's an example of the kind of challenge that we end up in. So we can't -- what we have been able and willing to provide in classified or in unclassified, and we've given this obviously, is the basically the backgrounds of various experts that we've consulted with, the actually published information that we've relied on and answer any questions about how we got to a contractor.

MICHAEL TURNER:

Director, I'm going to need you to conclude.

AVRIL HAINES:

Got it. And I'll just finish with the last thing, which is if there's anybody, sir, that you want us to talk to that you feel like we haven't, I commit to you that we will absolutely take those names and we will ensure that we are consulting with them as well.

BRAD WENSTRUP:

We're just trying to do the best job we can to in the future, be able to predict a pandemic, prepare for it, to protect the American lives and to prevent one if we can.

MICHAEL TURNER:
Mr. Carson.

ANDRE CARSON:

Thank you, Chairman and Ranking Member. This an open question. Last week our committee heard from several respected leaders from the think tank community and in their remarks, they presented differing views about whether a standalone open source agency is needed in the IC. What are your views? And what are your agencies doing to incorporate open source reporting and its analysis to help counter the threats described in your remarks?

AVRIL HAINES:

I'll just start, but I think going to Director Burns and to General Berrier would be useful for you to hear what they're doing because they are really centers of excellence in this area. We have been through a process whereby we've been trying to ensure that the open source work that is being done across the community essentially is as effective as possible in supporting the priorities across the intelligence community.

And one of those issues that's come up is how do we organize ourselves, how do we ensure we have the right talent, how do we ensure we're supporting the technology that's needed, and maybe maintaining the partnerships with the private sector and otherwise that are important to this effort. And we had an external panel look at that and we have received advice and we are going to be establishing at ODNI and OSINT Executive, which is a small group.

It'll be like a dozen folks if we go forward with this, basically to support the work that is being done across the intelligence community. The CIA is the functional manager for us on OSINT and the DIA is the defense intelligence enterprise manager on this. So I'll turn to them.

WILLIAM BURNS:

Sure. No, just to add, Congressman, I mean I take very seriously the increasingly important role of open source information. We can't function effectively as an intelligence service as the functional manager across the intelligence community unless we put more resources, more drive, more energy into this issue.

So I appointed a new director of our open source enterprise several months ago and I'm really pleased with the drive and energy and creativity that he's bringing to this as well, not only to make better use of artificial intelligence and machine learning. Because the challenge for us, for our analysts, is sifting through the avalanche of information that's out there, sifting through the haystack to get to those needles that are going to matter most to human analysts, human analysts and doing it very quickly and then to work with Director Haines and General Berrier and our other partners in the IC to avoid duplication.

So we're learning from one another's experiences. And then also I think to look at ways in which we can learn from one another on training, on governance issues as well. So I'm pleased with the progress we're making, but I'm determined to continue to drive this.

SCOTT BERRIER:

Congressman, we think that open source when combined with other sources of information that are classified really comprises the secret sauce for all source analysis. And so I would say from a defense portfolio side of the House, what we are trying to do is formally establish the defense program so that we have standards for training tradecraft that we're not getting ripped off in multiple places by buying the same kind of data and that we're doing this in a way that's smart across the services and across the combatant commands.

ANDRE CARSON:

Lastly, chairman, recently we heard from several speakers including General Petraeus, who warned of a lack of a genuine workforce development training in the IC. What are your organizations doing to improve diversity when it comes to recruiting and retaining your workforces? And if you agree that the IC needs to devote more resources to professional development, how do you all plan on tackling those very apparent issues?

AVRIL HAINES:

Yeah. Thank you very much, congressman. I think there is no question that we have to do better on diversity, equity, inclusion and accessibility. And I think you'll see in our budget requests and our proposals in all of the work that we're doing that we see this as an area that we need to focus more intense resources and efforts.

I will tell you that as a general matter, when I look across ODNI for example, in the senior leadership, and I look at the percentage of Hispanic and Latinos, for example, it is a little bit more than three percent, and that clearly does not reflect the country. These are things that we are trying to get out.

So the first part from my perspective is ensuring that we have data that is reliable, that allows us to be held accountable to what our diversity and inclusion is and that we're able to do barrier studies and work that allow us to understand where there are challenges. We are also working across a range of other issues that we've seen to sort of promote recruitment across the country in a variety of different communities to ensure that we're reaching folks that don't normally come to the IC or know about the IC, that we are focused on retaining the diverse talent that we do have.

We've recently looked at a project that we hope to --

MICHAEL TURNER:

Director, I'm going to have to ask you to summarize.

AVRIL HAINES:

Sorry.

MICHAEL TURNER:

In order to get through the list that we have and we're going to have to close the list. We're going to have to start keeping everyone to the five minutes. So if you'd make your answers just a little bit shorter so we can get to everybody and get to the closed session.

AVRIL HAINES:

I'll stop here and we'll proceed.

MICHAEL TURNER:

Okay. All right. Do you yield?

ANDRE CARSON:

Thank you, chairman.

MICHAEL TURNER:

Thank you. Mr. Stewart.

CHRIS STEWART:

All right. I'm going to talk really fast. There's a couple of things I do want to talk about. And again, to hit them both, I'm going to be very brief on the first one and that is 702, to reemphasize the importance of that. Thanks for all of you being here. We recognize that each of you are distinguished leaders.

If I could make this point in introduction to 702, all of us are responsible to the people, but those of us sitting up here have a special responsibility to the people. We go home every weekend, and we talk with hundreds of people. I think we have a pulse on where the people are far more than the executive, far more than military or intelligence officials and I would say far more than the Senate.

And so I think we have a pulse of the people. And in that regard, then when we talk about 702 and the fear and concern they have, Director Wray, if I could, I'm going to read you a communication I had from a constituent who is a national security expert official and then I'd ask you to respond or maybe you don't want to. But I read this to you to illustrate this is the challenge we have when it comes to reauthorizing.

And much of this is shared by members of Congress as well. But quoting from him, we could show dozens of examples, sending FBI agents to shut down local prosecutors for going after Jeff Epstein, systemic abuse of FISA, systemic abuse of First Amendment rights, targeting parents and Catholics, refusing to investigate multiple reports of sexual abuse of US gymnasts.

The problem is, speaking of the FBI, they have no accountability, near absolute power, and they know no one, not even Congress can touch them. That is what many, many Americans feel. And now we have

to go to them and say, yeah, we understand your concerns but at the same time, we want to reauthorize these powers and authorities.

I read that for you as we discussed earlier, as a challenge we have. You're welcome to respond to it, although please do so briefly or if you just recognize, yeah, we need to admit to the American people that we've made mistakes and we're going to correct it.

CHRISTOPHER WRAY:

So congressman, I appreciate you sharing your constituent's letter with me. What I would say is, of course, like any major institution, we have made mistakes. Some of the descriptions in the constituent's letter are not accurate, in terms of what actually happened. But absolutely, we have made mistakes. And to me the mark of a leading organization is not whether it makes mistakes or not.

All major organizations, all elite organizations do, but whether or not we learn from those mistakes. And I think we have, and we've made all sorts of changes, which I could go into on different issues, but we're determined to be worthy of all Americans trust, including your constituents.

CHRIS STEWART:

Well, and I appreciate that because that's where we're going to find success, is if we can say that we recognize that we can do better. And to do better, the process has got to be reformed somewhat. And we look forward to working with you because we do have to reauthorize 702. Director Haines, this is to you.

I think you're probably most appropriate to answer this. I mean, there's so many things we could talk about here. We look forward to the closed hearing as I said, but we have to talk about China. I reflect back on my military experience. There are a number of incidents. A couple of times when we had American assets, American intelligence aircraft who were captured and had a forced landing in China.

The P3 incident with the JA is an example. And during that time, we didn't really know what our policy would be, how the US would respond. In the past, the president has said pretty clearly that we would respond with military action if China were to invade Taiwan. And then shortly after that, the administration kind of walked back those comments, but it didn't occur just once, it occurred several times.

We have this policy of strategic ambiguity, which has served us well for the last 30 years. But I wonder if it's not time for us to declare another policy, a new policy and that is we will defend Taiwan. It's pretty clear the president seems to think that. And I think if we're going to deter, again, understanding the need for strategic ambiguity before, but times are different now.

If we're going to deter, I think we have to be clear in saying yes, we will defend Taiwan militarily if we have to. Director, am I wrong? And and has there been a change in the administration's policy regarding ambiguity?

AVRIL HAINES:

Thank you, congressman. Obviously not in a position to comment on policy, but I certainly -- I think you're right in recognizing the president's comments on this issue and that that has been a pretty strong statement.

CHRIS STEWART:

Okay. So let me in the 13 seconds I have, do we agree that there would be a stronger deterrence if our adversaries knew that we would defend militarily if necessary?

AVRIL HAINES:

You mean sort of -- in this particular case, I think it is clear to the Chinese what our position is based on the president's comments.

CHRIS STEWART:

Thank you, and I only went ten seconds over, Mr. Chairman, so I yield back.

MICHAEL TURNER:

Very good. Mr. Krishnamoorthi.

RAJA KRISHNAMOORTHY:

Great. Thank you, Mr. Chair, and thank you Mr. Himes for unearthing evidence of free snacks at the NSA. We'll be visiting shortly, General Nakasone. My first question is directed to Director Wray. Mr. Wray, you've said that TikTok, the popular app on people's phones is quote, a tool that is ultimately within the control of the Chinese government and it screams out with national security concerns, close quote.

We found that TikTok and ByteDance employees regularly engage in a practice called heating, in quotes, heating a manual push that ensures specific videos, quote, achieve a certain number of video views. Mr. Wray, can you rule out that TikTok has heated content at the direction of the CCP?

CHRISTOPHER WRAY:

I don't think we could rule that out.

RAJA KRISHNAMOORTHY:

Can you -- now, let me just talk about another instance of what I think is very problematic behavior at TikTok and ByteDance, their parent company. In December of last year, ByteDance confirmed it used TikTok to monitor US journalists, physical location using their IP addresses in an attempt to identify whether they had been located by ByteDance employees.

Can you rule out that this data was also shared with the CCP?

CHRISTOPHER WRAY:

I don't think we could rule that out.

RAJA KRISHNAMOORTHY:

Could the CCP use TikTok to shape political opinion such as to misinform the American public?

CHRISTOPHER WRAY:

What you just described there is one of the concerns that we have, namely that the control of the recommendation algorithm could be used to conduct influence operations. And much along the lines of your first two questions, it's important to understand that that's not something that would be easily detected or ruled out, as you say.

And that's just one of several security concerns that we have about TikTok.

RAJA KRISHNAMOORTHY:

Thank you. Director Haines, recently my staff described to me a term called Guanxi. Apparently, Guanxi is a Chinese term that refers to a part of Chinese culture where people develop personal trust and a strong relationship that can involve moral obligations and exchange of favors. And they suggested -- in the press there have been suggestions that guanxi has developed between Chairman Xi and Vladimir Putin. Let me ask you this question.

Do we have any evidence that, in Chairman Xi's calculations of potentially providing military assistance to Russia in Ukraine, that he has ever discussed or he has discussed among his internal cadres potential assistance by Russia to China and the PRC in a potential invasion of Taiwan.

AVRIL HAINES:

Thank you, Congressman. I think maybe we could discuss this in closed session.

RAJA KRISHNAMOORTHY:

Okay, very good. General Berrier, I want to talk to you about something called peace disease, which has -- Chairman Xi has talked about repeatedly in his speeches recently. This is what a former general of the Central Military Commission in the PRC has described as peace disease. He said, quote, "Today the PLA hasn't been in actual combat for many years, yet the fires of war are burning throughout the world.

In this area, the gap between the PLA and foreign militaries is growing day by day." And then he closes with the quote, "This is an actual problem," close quote. This was a quote from two -- a 2009 speech by the general of the Shenyang military region. This term, peace disease, refers to supposedly a lack of combat readiness on the part of the PLA, has appeared 565 times in the PLA Daily between 2012 and mid 2018. And just recently, Xi Jinping said he wants to cure the peace disease.

How do you assess when Chairman Xi would know that the peacetime disease has been cured and that their troops are ready for combat?

SCOTT BERRIER:

I'm not sure that we could actually put a -- a fixed date on that. We know there are a few dates out there like 2027, 2035, and 2049, and we know that his -- his leaders don't have the kind of combat experience that, say, the -- the American military leaders have. So, we -- we think that this is in his mind and perhaps shapes the way that he thinks about -- about the readiness of his force.

And we could probably go into a few more details on that in a closed session.

RAJA KRISHNAMOORTHY:

Very good. Director Burns, I wanted to ask you a question about threats from ChatGPT, but I just couldn't think of any. So, I went to ChatGPT and I said ask question of CIA Director Burns about threats from ChatGPT. It said Director Burns, what measures is the CIA taking to monitor and mitigate potential risks associated with the use of AI language models like ChatGPT, and how would you prevent AI language models not to be used by malicious actors to spread false information or influence public opinion?

That's from my pal, ChatGPT.

WILLIAM BURNS:

Sure. And I'm -- I'm glad to give you an example which I'm sure ChatGPT is very well aware of. And that is that, you know, if you assume, say, a foreign -- an adversarial intelligence service, where English is not the first language and they're thinking about ways in which they could come up with compelling spear phishing messages, it's logical to use artificial intelligence of one -- one kind or another to produce a message that can be pretty effective in spear phishing, and therefore in taking advantage of vulnerabilities.

And so, what we're working on with colleagues across the intelligence community are ways of identifying, you know, when that kind of spear phishing effort is being made using artificial intelligence by a foreign adversary.

RAJA KRISHNAMOORTHY:

Thank you.

MICHAEL TURNER:

Mr. Crawford?

RICK CRAWFORD:

Thank you, Mr. Chairman. Thank you all for being here today. I've got a Wall Street Journal report I want to -- I want to refer to here. It was published earlier this week, detailing how unprepared, in their view, America is for an era of, quote, great power conflict with the likes of China and Russia.

Here are -- here's a little bit of their analysis here. Quote, decades of ever bigger military budgets, including a seven percent boost in spending this year, have improved the lethality of China's air force, missiles, and submarines, and better trained -- better training has created a more modern force from what was once a military of rural recruits.

China is developing weapons and other capabilities to destroy an opponent's satellites, the Pentagon says, and its cyber hacking presents a threat to infrastructure. Further, a similar report from the Australian Strategic Policy Institute published findings around countries who are leaders in advanced technologies, 44 categories measured.

Of those 44 categories, the United States led in seven. China led in the balance. I have that graph. I'd ask unanimous consent to enter into the record.

MICHAEL TURNER:
Without objection.

RICK CRAWFORD:
China's research -- the study said, quote, China's research strengths at the intersection of photonic sensors, quantum communication has advanced optical communications, in addition to post quantum cryptography -- cryptography could mean that intelligence communities, particularly the Five Eyes, could lose important capabilities and suffer from diminished situational awareness.

China leads globally in photonic sensors, quantum communications, advanced optical communications, and post-quantum cryptography. It further states, taken together, these observations increase the risk of Chinese communications going dark to the efforts of Western intelligence services. This reduces the capacity to plan for contingencies in the event of hostilities and tensions," end quote.

Let me ask you, panel, do you agree or disagree with those statements? And what is -- your agency or agencies, what are you doing to build, catch up, or stay ahead of China considering those comments?

PAUL NAKASONE:
Congressman, if I might begin, I would agree that China has shrunk the gap in terms of where they were previously to where they are today. What is the National Security Agency doing? Several things. First of all, we play to our competitive advantages. We make code and break code better than anyone in the world.

The second piece is that we look at partnerships. You mentioned the Five Eyes, but it's a broader set of partners that we have to bring in, academic partners, engage with industry, engage with allies. This is what gives us strength that China will never have. And the last piece is the close association that we have as a combat support agency with the Department of Defense to identify vulnerabilities, mitigate them, and then ensure that we can advance from them.

SCOTT BERRIER:

Congressman, the Defense Intelligence Agency has recently reorganized with a China mission group that is specifically focused on this threat. We're continuing to engage our Five Eyes partners and other partners in the region on where we can -- where we can work together to -- to get after this threat in a collective way.

And we will be expanding our footprint into the Indo-Pacific here very, very soon.

RICK CRAWFORD:

Excellent. Thank you. Any further comments?

WILLIAM BURNS:

Sure. Sure. Just -- I mean, we've done -- made the same kind of important organizational changes, because I think the two challenges that you just talked about, Congressman, are going to be central to our futures as an intelligence service, meaning China and competition with the PRC, and then the revolution in technology, which is going to be the main arena for that competition.

So, what we've done is stepped up considerably our efforts to collect on all the areas that you described, stepped up our efforts working with partners in the US government, but also foreign partners as well to slow down PRC's efforts to try to, you know, gain an advantage in those areas. And then just to underscore what General Nakasone said, what's crucial to all this is working with partners, both in the private sector as well as foreign partners as well.

RICK CRAWFORD:

Excellent. Let me flag one more issue for your attention. This is also a Wall Street Journal report. A remote corner of Taiwan confronts wartime scenario, that's the headline, life with no Internet. And the - - and the gist of this is there's a -- there's an island that had their Internet cut off, effectively, and -- and this is typically a precursor for kinetic action.

And the question I have is, with regard to Taiwan, do you think we have adequate redundancies to be able to address that threat should that situation arise?

AVRIL HAINES:

I think I'll just say generally this is an issue that we're worrying about across all partners, allies, et cetera, is to ensure that we have a way to help them. And I think we can, yeah, further discuss details.

RICK CRAWFORD:

So, that's been the case in Ukraine, where obviously that was --

AVRIL HAINES:

Exactly.

RICK CRAWFORD:

Diminished their capability for communications and so on, operational control. And that's why I asked the -- the question, because I obviously have some concerns about addressing that. Do we have the adequate resources in place to -- to mitigate that threat? Thank you. I yield back.

MICHAEL TURNER:

Mr. Crow.

JASON CROW:

Thank you, Mr. Chairman. Russia has committed and continues to commit unspeakable war crimes against the Ukrainian people during the conduct of this war. The United States is not a signatory to the International Criminal Court, but Congress last year passed a law that made it very clear that we should provide intelligence and information related to these crimes to the International Criminal Court.

And I will quote, in the appropriations bill that passed late last year, it allows exceptions allowing for assistance with, quote, "investigations and prosecutions of foreign nationals related to the situation in Ukraine, including to support victims and witnesses," end quote. And of course, the discussion around that and the debate around that made it very clear that Congressional intent was for the IC to provide that information to the ICC. It's my understanding that there's debate within the administration, more specifically that the Department of Defense is preventing that assistance and that information from being relayed to the ICC, including a principals' meeting that occurred on February 3rd where there was debate about that.

So, Director Haines, it is your -- is it your understanding that current law passed by Congress mandates the ICC provide, or the United States -- the IC provide this information to the ICC in furtherance of investigations of Russian war crimes?

AVRIL HAINES:

Thank you, Congressman. So, we absolutely -- and I don't think there's any debate that we should be providing support to the ICC on Russian war crimes, you know, as a general matter. The -- what -- what we do is we provide intelligence that can be provided to the ICC through the arms of the US government that typically work with the ICC, so the State Department's War Crimes Issues Office.

We don't do that directly. And -- and I think, you know, it's really a question for them as to what exactly they're providing and whether or not --

JASON CROW:

So, is it your understanding, Director, that there is information that is currently not being provided to the ICC that the intelligence community would like or otherwise would provide to the ICC that the -- the Department of Defense and this administration is not allowed to be provided?

AVRIL HAINES:

No.

JASON CROW:

So, there's -- there's no dispute about that within the administration?

AVRIL HAINES:

I don't -- we provide it to the policy arms. They provide it to the ICC. I don't actually know exactly what they have provided that --

JASON CROW:

So, more specifically then, is it your understanding that the Department of Defense is holding up the provision of information or intelligence to the ICC?

AVRIL HAINES:

No.

JASON CROW:

It's not -- that's not your understanding.

AVRIL HAINES:

It's not my Understanding. I think --

JASON CROW:

Director Burns, do you -- do you have an understanding one way or the other on this?

AVRIL HAINES:

No, same as Director Haines on that -- on the question you asked, sir.

JASON CROW:

Okay. The next question is about the -- the assistance generally to Ukraine. There's a lot of debate within Congress right now and -- and with the administration about the -- both the quantity and the quality of the military assistance to Ukraine. My understanding is that Russia does not have the capability of any major offensives or breakthroughs currently in Ukraine, that they've been degraded sufficiently.

So, Director Burns, is that your understanding, that in 2023 that the Russians couldn't conduct major offenses or have major strategic success in Ukraine?

WILLIAM BURNS:

Yes, sir. It's our judgment that the Russian military is capable of making incremental tactical gains, and they made some in the course of the offensive they've launched over the last four or five weeks in the Donbas in eastern Ukraine. But it is our collective assessment, I think, that, for a whole variety of reasons that Director Haines mentioned, munitions shortages, morale problems, manpower problems, conflicts within their own military leadership, that they're unlikely to be able to make significant strategic breakthroughs or sustain them over the course of the rest of this year.

JASON CROW:

And is it your understanding that Vladimir Putin's strategy is to recapitalize the military to consolidate support and to rebuild his infrastructure so that he will be capable of making advances or strategic success within 2024 and 2025, that he's taking a longer term view?

WILLIAM BURNS:

Yeah, I think Vladimir Putin is very much taking a longer term view. I think he's doubling down in -- in many respects right now. I believe he's convinced that he can make time work for him, that he can grind down the Ukrainians through this war of attrition, that he can wear down Western supporters of Ukraine.

And he's convinced also, and has been for some time, that Ukraine matters more to him than to us. Therefore, the challenge, I think, is to puncture that view.

JASON CROW:

So, given that -- that decisions have to be made about relative risks and where risks lie, short term risks versus long term risks, would it be your best advice that we transition the nature of our support to look more towards hardening Ukraine and military modernization efforts that would look further out in the horizon than the shorter term efforts?

WILLIAM BURNS:

Well, I -- you know, I avoid offering free policy advice in my current role these days. What I would say as a matter of intelligence assessment is that the next several months, the next four, five, six months, are going to be crucial on the battlefield in Ukraine. I think any prospect for a serious negotiation, which President Putin I do not believe is ready for today, is going to depend on progress on the battlefield.

Therefore, I think, analytically what's important is to provide all the support that we possibly can, which is exactly what the president and our Western allies are doing for the Ukrainians, as they prepare for a significant offensive in the spring. And then at the same time, it's not really an either/or question, just as you said, Congressman.

It's looking at the long term security needs of Ukraine to help ensure a situation where Vladimir Putin's Russia is not going to try to mount another offensive or another invasion, as they did at the beginning of last year.

JASON CROW:

Thank you. I yield back.

MICHAEL TURNER:

Ms. Stefanik?

ELISE STEFANIK:

Director Wray, one year ago at this very same hearing, I asked you about the deadliest vehicle crash in decades in my district in upstate New York, the 2018 Schoharie limo crash, instantly killing 20 people. Those families have never been the same, and my office has communicated with many of them. The owner of the illegally retrofitted limo was a longtime FBI informant with a rap sheet a mile long. And it was because of my question to you in this open hearing that the FBI was forced to open an internal review. Let me be clear. That review was in response to our congressional oversight. Since then -- that was a year ago -- the FBI has stonewalled and slow walked our additional requests for updates on that review until miraculously just this week before you knew you were going to appear here today, we received an email informing this committee and myself of the following.

The internal review is now complete. The FBI will provide a briefing and in connection with that briefing we will make available the internal review with certain redactions. We'll coordinate with your staff regarding the in-camera review of the materials. The FBI is providing this briefing and materials with the understanding that the committee will not publicly disclose the nonpublic information contained therein.

My expectation is that briefing will be this month. Do I have your commitment?

CHRISTOPHER WRAY:

Yes.

ELISE STEFANIK:

I want to follow up. Can you commit to providing that briefing to those family members, immediate family members, the parents or spouses of those victims?

CHRISTOPHER WRAY:

On that one, let me make sure I talk with our folks and circle back with you about what can be shared if there are any limitations. Obviously, we want to make sure that the victims and their families are appropriately informed, but I don't know yet what constraints there may be. So we will follow back up with you on that.

ELISE STEFANIK:

Yeah, they have not been appropriately informed and it's only because of my work in congressional oversight that they're starting to have sunlight. I believe you're a parent, Chris Wray.

CHRISTOPHER WRAY:

Yes, I'm a parent.

ELISE STEFANIK:

I'm a new parent as well. And these -- there is a set of parents that lost three daughters in that crash. So providing sunlight and transparency is important. I also want to note an important portion of the letter that was included. It says the FBI considers the provision of the internal review as fulfillment of the above referenced fence.

I remind you that this committee, not the FBI, determines the level of transparency equating to full compliance with our constitutionally directed oversight role. Mr. Chairman, I want to submit this unclassified version of the letter for the record.

MICHAEL TURNER:

So ordered.

ELISE STEFANIK:

I also want to shift gears here regarding Judiciary Committee. I serve on the select subcommittee there. And this committee has made 50 different requests for information and documents concerning the operations and the actions of the FBI. And to date, the FBI has not complied with the Judiciary Committee's long outstanding requests for information and documents.

The FBI is accountable to Congress and by extension the American people. Responding to this routine oversight is the bare minimum. And today, the FBI failed to send a witness to the Judiciary Committee hearing saying that we had this hearing happening. Can you commit to sending a witness before the next Judiciary Committee subcommittee hearing on March 28th?

CHRISTOPHER WRAY:

We're happy to work with you on making sure we make the information available.

ELISE STEFANIK:

Can you commit to provide a witness?

CHRISTOPHER WRAY:

We will of course make people available to the committee.

ELISE STEFANIK:

But you didn't make people available today. This is the base minimum. The agencies need to provide witnesses. Can I get a commitment, yes, you will provide a witness?

CHRISTOPHER WRAY:

We will work with you to make people available.

ELISE STEFANIK:

That's not a yes. So for the American people, you are having the FBI director refuse to provide a witness. Just say yes.

CHRISTOPHER WRAY:

I'm not refusing to provide a witness. I want to be clear on that. I said we will work with you to make somebody available.

ELISE STEFANIK:

So great. So someone will be made available?

CHRISTOPHER WRAY:

Yes.

ELISE STEFANIK:

Yes. Thank you. That's all I wanted, a yes. Moving forward, do you believe the Hunter Biden laptop story is disinformation?

CHRISTOPHER WRAY:

Well, I want to be careful about there is an ongoing investigation that is relevant to that. So I have to be careful about what I can share on that here.

ELISE STEFANIK:

Do you believe the Hunter Biden laptop story is disinformation?

CHRISTOPHER WRAY:

I don't think there's anything I can share on that in open setting.

ELISE STEFANIK:

Were you aware that the FBI personnel were in contact with Twitter regarding the Hunter Biden laptop story?

CHRISTOPHER WRAY:

I don't believe FBI personnel were in contact with Twitter about the Hunter laptop story specifically. I think there were people in contact with Twitter about Russian disinformation efforts.

ELISE STEFANIK:

Of which the Hunter Biden laptop story was included according to the FBI.

CHRISTOPHER WRAY:

Well, I don't know exactly what you're looking at, but I am happy to talk about what it is the FBI does and does not do with respect to social media companies.

ELISE STEFANIK:

Were you aware that the FBI had Hunter Biden's laptop since December of 2019?

CHRISTOPHER WRAY:

I can't speak to exactly when we had a laptop available. There is a -- as you know, there is an ongoing investigation run by the US attorney out of Delaware from the prior administration that we continue to work very closely with. And our Baltimore --

ELISE STEFANIK:

-- And we had an ongoing investigation as well.

CHRISTOPHER WRAY:

And our Baltimore field office is working very hard with that US attorney and I expect them to pursue that case as far as it takes.

ELISE STEFANIK:

This stonewalling, Director Wray, the American people deserve answers, and this is unacceptable. Lastly, did you sign off on the Mar-A-Lago raid?

CHRISTOPHER WRAY:

Well, first off, it was not a raid. It was an execution of a search warrant.

ELISE STEFANIK:

Did you sign off on the execution of the search warrant?

CHRISTOPHER WRAY:

May I finish? Second, I don't sign off on individual search warrants in that case or in any other.

ELISE STEFANIK:

Did Attorney General Merrick Garland sign off to your awareness?

CHRISTOPHER WRAY:

I can't speak to the attorney general.

ELISE STEFANIK:

Was there dissent at senior levels of the FBI about the conducting of the -- of the search warrant?

CHRISTOPHER WRAY:

I can't speak to internal discussions among the FBI or among the FBI and the Department of Justice.

ELISE STEFANIK:

Even though it's been reported in The Washington Post.

CHRISTOPHER WRAY:

There are lots of things reported in the media all the time.

ELISE STEFANIK:

I know. Leaks from your agency. Leaked from your agency frequently it's reported in the Washington Post.

CHRISTOPHER WRAY:

It may or may not be accurate.

ELISE STEFANIK:

It may or may not be accurate. With that, I yield back.

MICHAEL TURNER:

Thank you. Dr. Bera?

AMI BERA:

Thank you, Mr. Chairman. In preparation of this briefing, staff gave me a number of questions to ask. And then lo and behold, yesterday we got an email from the speaker and Leader Jeffries talking about a

data breach at DC Health Link that affects all of us. We all got that. So let's talk about cybercrime, ransomware, et cetera.

You have to -- I'm sure we will get briefed on the data link in the future. But obviously, cybercrime and ransom wear is a major issue that we're dealing with and probably becoming much more frequent. Maybe this is a question for Director Haines or Director Wray. I was prepared to ask about state actors, but also non-state actors.

We can harden all of our devices, harden all of our offices, but there are lots of weak links out there. And I think a couple of things. How do we work with the private sector to compel them to put in the resources to harden their cyber hygiene? Number two, how do -- and maybe this is for Director Wray or either one of you.

For private sector companies, small and large ones, how do we compel them to make sure they're working with us, whether it's the IC or the broader community to let us know when the ransomware occurs? And because you know for us to address this issue, we have to be aware of the issue and we have to get that information.

So, to whoever is appropriate.

CHRISTOPHER WRAY:

So you're exactly right in one sense in particular that the private sector is the key to all of this. Eighty-five percent of our critical infrastructure is in the hands of the private sector. It's probably a higher percentage of that when you look at our innovation and an even higher percentage than that when you look at our PII. As you know, Congress passed, which I think is an important first step, a breach notification bill that will reach critical infrastructure.

In particular, I think there are things that can be done and should be done to strengthen that to ensure that the information not only is flowing from a broader swath of the private sector, but also is flowing more quickly to us so that we can help as quickly as possible. And then I think overall part of it is raising cybersecurity awareness, which is part of what the really active engagement that we're trying to participate in, all of us, with the private sector is designed to accomplish.

PAUL NAKASONE:

If I might add, congressman, it also means being able to leverage what we do as an intelligence community, operating outside the United States, understanding what adversaries are doing, being able to see their tradecraft, being able to share that tradecraft publicly. This is back to the partnership that is very close between NSA and FBI in terms of when we see certain things happening there, being able to provide that to the FBI as they talk to US critical infrastructure companies in the United States.

And we prioritize that work. That's very, very critical to us.

AMI BERA:

Great. Thank you. Let me shift directions. A couple of weeks ago, I had a chance to go on a bipartisan to Japan in my foreign affairs capacity. And clearly, Japan is a geopolitical strategic ally of increasing

importance, and we applaud the Kishida administration for really stepping up and understanding the new framework.

Yeah. They brought up in our meetings, obviously, they're not at five eyes, but five eyes plus one et cetera. But as we started to talk about their cyber hygiene, the fact that some of their own laws don't allow them to do security clearances, et cetera, we want to have this relationship. We want to co-develop products.

And you know, what can we do as Congress? And then working with the administration to -- they're very aware of their vulnerabilities on cyber, but it seems like it's moving very slow. And I'd be curious.

PAUL NAKASONE:

So, congressman, I'd welcome to brief you and other members of the committee of what we're doing with Japan and other partners in the Pacific to, as you indicate, raise the bar for cybersecurity. I think this is instrumental to understanding where we need to go as both the intelligence community and select partners.

We need to be able to share information with the great assurance that they can protect it. We need to be able to communicate them with the idea that what we're saying will not be monitored. These are all things. And I give the Japanese great credit. Over the past several years, they have done tremendous work.

But we do need to focus on this very, very hard going forward.

AMI BERA:

Great. Director Haines, or anyone.

AVRIL HAINES:

Yeah, I'll just add to what General Nakasone said. I mean this is an area of work that we have been engaged with Japan, with the Republic of Korea. We've actually have a trilad through which we work together on these kinds of issues. It's incredibly important, as you say, just to build -- help all of us be better at cybersecurity, but then also to be able to work against, for example, North Korea, others that are engaging in activities that are attacking our systems.

WILLIAM J. BURNS:

And well, I would add, congressman, is that you know we share both the admiration for what Prime Minister Kishida and the Japanese leadership is doing now in terms of their national security, which is hugely important to our shared interests. And I think we also applaud the Japanese leadership for understanding, you know, what we've sometimes learned the hard way in the United States.

It's not as if we have a monopoly on wisdom on this, but the importance of improving cybersecurity as well. And as an agency, we're working with our partners. I was last in Tokyo in December, I guess talking about these issues to do as much as we can to be supportive as the committed allies that we are.

AMI BERA:

Great. Thank you. And I yield back.

MICHAEL TURNER:

Mr. Kelly.

TRENT KELLY:

Thank you, Mr. Chairman. And thank each of you for being here. And I want to start off. The men and women who do the work of the IC are amazing men and women and they protect this nation on a daily basis. However, I will comment on some of the things that have happened. There is an erosion of trust in the American public that you are protecting us and protecting all of our constitutional and civil rights that are created through the Constitution.

Whether that is leaks at high levels to the -- to media sources or to put a political viewpoint, which is not necessarily anybody at this table, whether that is resistance to oversight and using is currently under investigation. Just an understanding, we are not a normal congressperson. We are selected for this committee.

We have had trust in place by us by both sides of the aisle to be able to keep and maintain the same secrets that you do. There -- whether it's not providing witnesses when we ask for them and saying well, they may not want to be disclosed. We have subpoena power. If they don't want to disclose, we can subpoena them.

It is important for us to be able to do our job as partners with you in that oversight. And that is what we want to do, not to throw daggers and rocks at you. But what we want to do is we are the people who are most charged with selling FISA renewal to the Congress and to the American people. And without proper oversight, we can't do that.

As we used to say in the Army one, oh, crap does away with 10 years of atta boys, okay? I mean, we cannot do that. So when one leak happens, if the public doesn't feel like we're addressing that appropriately, we have to do that. So I would just ask you, Director Haines, what are we doing for you to help us rebuild the trust in the public that they have lost over the years?

Through -- many times it was -- it predates you, but it doesn't matter when it happened. We've got to turn the perception back that we trust the FBI. We trust the CIA. We trust the NSA.

AVRIL HAINES:

Absolutely. Thank you, congressman. I think having the trust of the American people from -- with respect to the intelligence community is absolutely fundamental. And it's critical to us doing our job for all of the reasons that you indicated, but also so that when we put out a warning, frankly, that the American people trust it enough to act on it or to be subject to it. And I'm -- so what we're doing is across the board trying to ensure that we have appropriate oversight over the extraordinary powers that we have.

In the context of 702, I think you've heard a little bit from Director Wray, but honestly all of us have a lot to say on the subject. Really, the investment that we're making in training, in policies, and procedures that help to ensure that we are doing things in accordance with the law that we are looking at designs of technology to ensure that it is actually quite hard to do anything else.

We are looking at the oversight process every two months.

TRENT KELLY:

Let me -- because I want to get a little more. I mean, you used the raids recently and raid, search warrants, whatever, all the documents through multiple presidents and vice presidents that were improperly disclosed. We've got to do a better job of not telling the American public all those things. But they have to know when the -- when the CPC asks for those things, and when we ask for those things and you tell us we don't have a need to know or a right to know, I can assure you that erodes public trust.

That does not help. We are not partisan folks on this committee when we are asking that. We are asking that for oversight. So I just ask that you comply with those. And the second thing, I'm going to shift a little bit to the southern hemisphere because I know in your Senate hearing, you talk quite a lot about the border and those kind of things.

TRENT KELLY:

We also talked about transnational terrorist organization and drug cartels and those things. That is not a kinetic fight. But I just asked you guys to look at what we -- as an intelligence community and a Title 10 community, what -- what can we do training assist wise to move to the southern border of Mexico south? What can we do to improve our standing in those nations?

Through training and assist or through intelligence provided to them, what can we do to strengthen our relationship so we don't have so much pressure on our border?

CHRISTOPHER WRAY:

I'll start and I'm sure others will want to weigh in. I mean, one thing that I would call out, you rightly said Mexico and then further south. So, one of the things that we've been doing that I think we can double down on, and we're trying to do that, is work with the Northern Triangle countries, you know, where we've got MS-13, 18th Street gang, etcetera.

But to illustrate how thorny and complicated this problem is, we have what we call transnational anti-gang task forces in all three of El Salvador, Honduras, Guatemala. And in El Salvador recently, for example, working with them, we had a massive MS-13 takedown, which was great. In the one hand, you got all these people locked up in El Salvador before they got anywhere near the border.

The problem is there's so many of them that the ones that didn't get caught immediately started fleeing, looking for someplace else to go. And guess where they wanted to come? They're heading straight for our border. So, it illustrates why we can't just kind of play whack a mole. We have to try to have a comprehensive solution to this problem.

TRENT KELLY:

And Mr. Chairman, I yield back.

MICHAEL TURNER:

Great. I'm going to ask unanimous consent that we go to four minutes, not three, but four in order for us to be -- to get done to make it to our one o'clock. Miss Spanberger?

ABIGAIL SPANBERGER:

All right. Thank you so much, Mr. Chairman, and thank you to everyone who's here. I proudly serve so many members of the intelligence community as their representative in Congress. And so, on that note, I'd like to start with something that has impacted personnel. I'd like to begin by --

MICHAEL TURNER:

Can we reset the clock, please?

ABIGAIL SPANBERGER:

By saying that I appreciate the outreach that I have received from various agencies knowing of my interest in this, and -- and the conversation hopefully will continue in closed session. But in this unclassified document, I'd like to just ask for comments on the fact that it literally says what to me are somewhat contradictory statements in one paragraph, noting it is unlikely that a foreign actor, including Russia, is conducting a sustained worldwide campaign involving hundreds of incidents, it continues, related to anomalous health incidents.

Further in the paragraph, it says the IC continues to actively investigate the AHI issue, focusing particularly on a subset of priority cases for which it has not ruled out any cause, including the possibility that one or more foreign actors were involved. There's a lot of consternation among those who have been impacted by AHI. I appreciate the work that you all are doing in making sure people are having their health needs met.

But would anyone like to comment on what appears to be, by my reading, somewhat contradictory statements in one small paragraph?

AVRIL HAINES:

Okay, I'll start. No, thank you very much, Congresswoman. I think there is no question while, as you're -- the analysis that you're looking at indicates that -- that is a general matter, you know, across the IC, most IC elements now have concluded that it is very unlikely that a foreign adversary is responsible for the reported AHIs, and there are different degrees of confidence associated with that.

And then you have some that look at it as unlikely that a foreign adversary, essentially, had done this part. At the same time, and this is sort of where, you know, our work continues, and there's no question that -- that we see this as a continued priority for us, is that we are going to be and continue to be

vigilant about looking for information that undercuts those assumptions, because we recognize there are gaps here.

We are going to continue to focus on trying to understand essentially what it is that we can do to help the folks that have experienced these very real symptoms and these issues, and to figure out what's happening to each of them. And as we look at the experts' panel that went through process to look at different mechanisms that might in fact be causing different symptoms, issues, and so on, they had recommendations on research and development that would continue to go forward, and that is something that we are also pursuing.

And any remaining questions that we have are things that we are looking to try to ensure that we're focused on being forwarded potentially --

ABIGAIL SPANBERGER:

So, we -- we're currently at a point, is it correct to say, where this is a point in time analysis, and the door is very much open and the investigation very much continues, that there could be a reversal or not of new information that would cause a new assessment that might differ from what we've seen thus far?

WILLIAM BURNS:

Yeah, I guess what I would say, Congresswoman, that first I have huge respect for your service at the agency as well, and to the intelligence community. And I'd say several things. Yeah, none of us are pretending that I think the thorough and rigorous work that was done reflected in the intelligence community assessment is -- none of us are pretending that that's absolutely the final word in this.

ABIGAIL SPANBERGER:

Good.

WILLIAM BURNS:

We will -- we will sustain a dedicated unit of officers at CIA, working with our partners in the intelligence community, not just to be alert to any new leads that could develop, but to follow them rigorously. We will also continue to focus with our partners on research and development efforts by our adversaries that could focus on directed energy mechanisms as well.

The only things I would add is, first, from the day I began as director of CIA more than two years ago, I've understood, I've tried hard to understand the significance of this issue. It's not an abstraction. It's about real people suffering, you know, real health conditions and real pain in the service of their country.

And so, we made fundamental improvements in the level and access to care. They will not diminish. We remain committed to, you know, supporting all of our workforce as well, and we'll continue to do that.

ABIGAIL SPANBERGER:

Thank you. If I may pivot quickly, because I will want to continue the conversation related to this in closed session, related to fentanyl trafficking, which is impacting communities across the country but certainly in -- within Virginia, can you update the committee on your efforts to combat cartels and the trafficking of fentanyl that we have seen to be so lethal within the United States?

WILLIAM BURNS:

I'd be glad to start Congressman, and -- and -- Congresswoman. I'll bring this back to the 702 issue too, because it has been a crucial tool in our efforts at CIA to collect foreign intelligence and enable our partners, whether it's in Mexico or our domestic partners in the United States, to take action to help protect Americans against the fentanyl crisis.

I'll give you a couple of broad examples, anyway. One is we've -- we've -- first, I should say we've transformed our approach at the agency to how we look at this issue to focus on networks, meaning precursor chemicals, financial flows, you know, the --

ABIGAIL SPANBERGER:

Precursors coming in from China, where else, going to --

WILLIAM BURNS:

From China and elsewhere, and -- and then also fentanyl, you know, production and processing equipment as well. 702 has been crucial in illuminating that network for us and therefore enabling us, for example, just in the last few months, to work with Mexican partners to take some very successful actions against the Sinaloa cartel, and then also in another instance, enable us to work with other partners to take significant action against fentanyl production and processing equipment in Mexico and in the United States.

ABIGAIL SPANBERGER:

Degrading equipment in those networks?

WILLIAM BURNS:

Yes.

ABIGAIL SPANBERGER:

Thank you for that update. Mr. Chairman, I yield back.

MICHAEL TURNER:

Mr. Fitzpatrick?

BRIAN FITZPATRICK:

Thank you, Mr. Chairman. Thank you all for being here and for your service to our nation. I just wanted to ask one question for the panel. It's my personal belief that the biggest challenge facing the intelligence community and therefore the biggest potential threat facing our nation is when, unlike 9/11, where we had universal 100 percent support, we had incredible bipartisanship here in Congress, incredible universal support for the intelligence agencies, when things happen -- and by the way, in the case of -- of Director Haines, Director Burns, Director Wray, due to the actions of your predecessors, not yourselves, you've been forced to deal with their actions -- when there's a chipping away of that trust.

There's -- when we're impaneling juries and -- and conducting jury questioning, there's a way to remove jurors for bias amongst other things. The background check system, the polygraphs can screen for drug use, foreign contacts and the like, but there's really no way that I'm aware of, and I don't know if there's a policy solution, that we can check for bias.

Because I think the biggest threat to these agencies is when there's a public perception that there's a political bias on the left or the right. It could be both. It used to be easy to do that when we lived in different times, but our country is very -- you know, hyper partisanship is at a spike right now, and that invariably bleeds into the hiring process and makes it tough for the agencies to screen for that.

So, how do you deal with that, right? I mean, when I was in the bureau, we've rarely, if ever, heard any talk about politics. We really didn't, and I took that as a source of pride for the bureau. But this was before we've seen the spike in hyper partisanship. How does the -- how do your agencies combat that?

Because it really is a risk, because it bleeds into the public not having faith, in some cases justified, in some cases not, of the actions of the various agencies.

CHRISTOPHER WRAY:

Well, I -- there -- obviously, it's a complicated topic. One thing I will point to that we've done, because I think you're right to focus not just on actual problems which have occurred, but -- but appearances issues, perceptions, those things matter. And so, one of the things that we did is I ordered a stand down to focus on not just objectivity, but making sure that we avoided even the appearance of bias.

And so, I started in a way that you will, from your past experience, recognize as very unusual at the FBI. Instead of saddling the front lines with some new training requirement because of something somebody else somewhere did, I started at the top. So, I took all 250 or whatever it is of the SES'ers all the way from legat in Australia all the way to California, and made them all come to Quantico for a single day where the overwhelming message was back to fundamentals, the right thing and the right way, what they heard from judges.

Because a lot of what you're describing about -- is sort of trying to adopt more of the kind of mindset the judges have. They may have political backgrounds, but they put those to the side. They check them at the door when they take on the robe. We need to have that same kind of mentality. So, the point was to start at the top, with everybody at the top of the organization, make them take the medicine first, and then push it out to the workforce.

And we did it for the entire workforce.

AVRIL HAINES:

If I can just add to that -- oh, do you want to -- just to say that I think this is a critical issue. And I think, Congressman, you know, as you think about this, if you have ideas for us, please let us know. I -- I see this as, first of all, from a leadership perspective, setting the tone for a culture that makes clear, just as you described your prior experience in government, that politics have no place in the work space and in national security, that this is something that -- you know, I also as -- grew up as a civil servant in the government, and nobody asked me what party I belonged to. That was never an issue, and that's something that just has no place in our work.

And -- and I think we are looking, you know, as Director Wray's comments made clear, like across the intelligence community. All of us I think feel very strongly about setting that tone for culture and making sure that that's not an issue. I think the second piece for -- for the IC more generally is in fact engaging in greater transparency where we can.

And I think exposing our assessments, doing an annual threat assessment world hearing in an open forum as you've asked us to come back and do, trying to put out more of our products, trying to give an opportunity for the American people to see the work that we do, sort of -- you know, to give a little bit more insight into how it is that we do things can help.

And then finally, in the context of transparency, giving more of a sense of the rules within which we operate and do not. And that's something that we're continuing to try to push out, frameworks and ways of working and compliance things, to expose when we make mistakes and when we don't and why it is that we're -- what we're doing about it.

MICHAEL TURNER:

Director, we're going to have to move on, if you don't mind holding your comments. Great. Mr. Crenshaw?

DAN CRENSHAW:

Thank you, Chairman. And thank you all for being here. And look, I -- I think you're all very serious security professionals, intelligence professionals, and I think that most of this report certainly reflects that. But there is a glaring exception to that, and specifically in the section on climate change and environmental degradation.

Now, don't get me wrong. I think this is indeed an issue, but I address this issue on a very different committee, not here, and for very good reason. So, I have a simple question. What creates greater geopolitical instability? It is the -- is it the occasional severe weather event or is it energy insecurity?

In other words, the inability of nations to secure reliable and affordable sources of energy, which one creates more global chaos and therefore represents a national security threat to the United States? Is it one or the other or both? I suppose I'll direct that question, I'm sorry, but to you, Director Haines because you mentioned it earlier.

AVRIL HAINES:

No. Thank you, sir. I -- so --

DAN CRENSHAW:

One or the other or both? I -- because I have a lot to say on this. And I --

AVRIL HAINES:

I don't have a way of quantifying it for you. So, I'm happy to try to take that for the record if that's useful.

DAN CRENSHAW:

Okay. Let's assume, you know, try to say both or one or the other. But the report only says one. The report only says one. So -- but if it was both, then why wouldn't energy scarcity be mentioned as a global threat? Why isn't radical environmentalism mentioned as a global threat? The last few years have some pretty glaring examples, and I'm going to point them out in my limited time here.

In Sri Lanka, radical environmentalist policies led to the collapse of farming outputs and the collapse of a government. The same thing is currently happening in the Netherlands, where their entire pharmacy -- farming industry is under threat. In Pakistan, your report mentions some flooding, but says nothing of the hundreds of millions of people without power because of energy scarcity due to foolish green energy policies by the Europeans that have made natural gas so unaffordable in countries like Pakistan.

European energy prices have gone through the roof, and they now desperately import coal and wood to burn because they engaged in misguided green energy policies for years. The WHO estimates that three million deaths result per year from lack of clean cooking fuels, meaning they're burning wood or dung instead of fossil fuels like propane and natural gas.

DAN CRENSHAW:

These things are truly destabilizing to global security, but there isn't a section in this report about it. The report does say that it's other events that are a national security threat and that tensions will rise as developing nations request reparations from developed nations. Of course, the assumption is that all weather events are due to climate change. That's not science, by the way. It's an assumption and I wouldn't expect assumptions from senior intelligence professionals.

It's worth examining the actual science. Has anybody read the UN Intergovernmental Panel on Climate Change report, all 4,000 pages? Really? Okay. But let's assume you have. It's got some good data in it, actually. I like that report and it would help this report be more objective. For instance, it actually makes science-based predictions about what the true economic costs of climate change will be over the next hundred years.

It says the cost of climate change by the year 2100 will be a 4.5 percent reduction in global GDP from what it otherwise would be, not from what it is now, from what it otherwise would be. So if we go on our trend of growth, we'd grow global GDP by 450 percent. The cost of climate change, make that maybe 434 percent.

That is not a national security threat. I'm sure you all agree with that. The report also states that insured losses due to catastrophes and climate change have increased 250 percent in the past 30 years. That is a fact taken way out of context. It's misleading. And again, I wouldn't expect it from intelligence professionals because the obvious explanation is that there's more homes and more infrastructure built on coastal areas.

The truth is -- the facts are that the deaths from natural disasters have decreased 90 percent over the last 100 years. The truth is that the trend in accumulated cyclonic energy, a metric that captures frequency, duration, intensity of global hurricane activity, says no increasing in trends. In 2021, we had the fewest hurricanes since satellite tracking began 40 years ago.

NOAA modeling shows that hurricanes making landfall will decrease 25 percent as the climate changes. The UN report, the science that never says red alert, never says crisis, never says any of the stuff commonly used by climate alarmists. I'm running out of time. So I just want to summarize, if the chairman will let me. When we say this kind of stuff and we detract from the very important topics that you all have been talking about this entire time, we detract from that.

And it's even worse when we don't at least balance it with the more obvious threat of energy insecurity globally and the destabilizing effects that that creates. That's my problem with this report and I hope we fix it next time. And I yield back. Thank you.

MICHAEL TURNER:
Mr. Hill.

FRENCH HILL:

Thank you, Mr. Chairman. And thank the panel so much for being here in this important open testimony for the American people to hear directly from you. Appreciate, Mr. Wray, your candid responses to the questions. Director Haines, you started out in your statement and you were talking about the slowing in Chinese economic growth and you stated that China now faced some domestic economic challenges.

So I'd like -- what is your assessment of what those primary domestic economic challenges for the PRC are? What -- how do you assess that slowing that economic vulnerability in China?

AVRIL HAINES:

Thank you, congressman. I just -- I point to a few here. So one is these are sort of structural issues that I think are going to be a challenge for China moving forward. One is their population, basically their aging population. So they peaked in 2021 and last year they declined by 850,000 people. It's the largest decline in over 60 years.

And with a relatively low fertility rate, China's population will continue to shrink even as it ages. And this is going to reduce China's labor force and likely increase expenditures on age related health issues as they're going forward. I think a second piece of this that is sort of looking at the domestic migrant workers' wages in China in low skilled industries have more than doubled on average as the quantity of migrant labor from rural areas has actually declined.

And this has contributed to several major domestic and foreign firms' decisions to actually to relocate their firms from China to low wage -- lower wage countries such as Vietnam or to issue expansion plans in China, leaving large numbers of China's low skilled workers unemployed. And then furthermore, China is going to need to improve education and training really to better prepare its workforce.

And at least 100 million low skilled workers risk losing their jobs as a result of automation that they're pursuing. And vocational education to sort of upskilled, untrained rural labor faces really entrenched obstacles within China. So these are some of the issues that we're looking at that sort of make it a particularly challenging environment.

And we think they're going to continue to sort of pursue their, you know, statist economic policies so that state direction is a part of it, which will not be as efficient essentially in their moving forward.

FRENCH HILL:

Well, in a follow up to that, do you assess that in their last 15 years of extraordinary space and defense technology build up that that workforce is aging? In other words, it has a median age higher than our baby boom generation and therefore they even have vulnerability in their defense space technological base because they have an aging workforce there.

Or is that a younger than average workforce? What's your assessment there?

AVRIL HAINES:

I don't know the answer to that. I'll find out.

FRENCH HILL:

Thank you. Director Burns, in open-source information, there's a lot of conversation about how effective the crypto criminals in the -- in DPRK in North Korea are about stealing cryptocurrency from wallets around the world. And that's in turn many times their export earnings or what we know to be their export earnings.

I think they -- most of their earnings are stolen. So it's kind of hard to gauge what those might be. What is the United States doing to interdict and block and stop the illicit flows to North Korea through that mechanism?

WILLIAM BURNS:

Well, I appreciate very much the question and maybe we can go into this in a little more detail in a closed session. But as we discussed when you came out to headquarters, this is a significant priority for us right now. And I know it's shared across the intelligence community because the North Korean regime does look at just what you described as a way of sustaining itself of, you know, acquiring revenue as well.

So there are a number of things that we can do working with some of our allies to counter that, but I'd prefer to talk about that --

FRENCH HILL:

Well, thank you. I yield back, Mr. Chairman.

MICHAEL TURNER:

The list is currently Garcia, Waltz, Scott. Mr. Garcia.

MIKE GARCIA:

Thank you, Mr. Chairman. I want to thank the witnesses. This has actually been a very enlightening and frankly clarifying couple of hours for me, but I think in a most disappointing way. I've been personally baffled over the last two years about our southern border policies coming out of this administration where in the last year we had 30 times the number of people die as a result of fentanyl poisonings than folks died during the 9/11 event.

Today, more people in our country will die of fentanyl poisoning than Americans died overseas in one day of World War II operations. And what's enlightening to me is that we didn't spend almost any time on this topic today except for the questions that have been posed to you. I read the 39 pages of the ATA, the 15 minutes of your testimony, Director Haines, and really no mention of these things.

You talk about misperceptions of US policies when we are actually being actively invaded on our southern border right now as a result of this administration's policy. So what's clarifying to me is the fact that we're sitting here with five people with billets such as director of national intelligence, director of Central Intelligence, director of National Security Agent, director of Defense Intelligence Agency, and the FBI. And you guys aren't messaging this as the number one threat.

I look at your table of contents within the -- when -- within the threat -- the annual threat assessment. You got China, Russia, Iran, North Korea, climate change, health security, developments in technology, transnational organizations, global terrorism, and the like. And I agree with these topics, and I want to put a boot on the throat of Russia, China, North Korea, and Iran just as much as anyone else.

But this is -- it's a shame that the fact that these poisonings right now that you characterize as overdoses and the migration challenges, as you say Director Haines, which are not migration challenges, this is an active invasion of our southern border, are being characterized by this body. It's indicative to me that you are not briefing the president of the United States on these issues correctly and that you're not putting the proper emphasis on the fact that we are being invaded and Americans are dying at a higher rate than Americans died during World War II on a daily basis as a result of these policies.

That's why these policies haven't changed. Very clarifying to me today based on your testimony as well as the ATA. On a separate subject, Director Haines, I want to ask you -- well, first of all, I want to ask you what you mean by misperception of US policies when it comes to our southern border. And I'll let you address that as quickly as you can, please.

AVRIL HAINES:

Thank you, congressman. I apologize if I gave you a misimpression that we do not believe that counter-narcotics is a critical aspect of our work and that it is a priority for the intelligence.

MIKE GARCIA:

It's not counter -- not to interrupt. It's not counter-narcotics. It's security of our homeland, defense, of our southern border. That is not the priority. You didn't give me the perception. You've given the American people that perception and your annual threat assessment reflects that. And frankly, we'll look at your budgets.

I'm an appropriator within for the Justice Department. I'll look at your budgets to see if it reflects that priority here shortly. But sorry, go ahead and continue.

AVRIL HAINES:

No, I just want you to know that that is a priority from our perspective. I think from -- on the border, we actually, you know, obviously support and facilitate the United States government terrorism watch listing process. We have parts of our -- even in ODNI, NCTC, the National Counterterrorism Center serves as the US central and shared knowledge basically on known and suspected terrorists.

And we maintain tied and we do a lot of work to try to ensure that all of the intelligence we have is provided to our border agents and to the Department of Homeland Security for the work that they do.

MIKE GARCIA:

I'd like to reclaim the last 10 seconds. It's a priority. I would submit that it needs to be your number one priority. And as a mission right now, we are failing. This is a war that we are currently losing and at the rate of 100,000 American lives every year. So I'll defer my technical questions for the classified setting.

But thank you, guys.

MICHAEL TURNER:

Mr. Waltz?

MICHAEL WALTZ:

Thank you, Mr. Chairman. Just to build on Mr. Garcia's questions. Director Wray, if ISIS or al-Qaeda poison through chemical warfare 70 to 80,000 Americans, will we approach that as a law enforcement problem or a military national security problem?

CHRISTOPHER WRAY:

I think we would approach it as all of the above.

MICHAEL WALTZ:

You would use -- certainly we would use military assets, whether it's cyber, space, what have you. You would -- you have the authorization through the authorization use of military force to do so, correct?

CHRISTOPHER WRAY:

That's my understanding.

MICHAEL WALTZ:

You would also have the authorization to use military resources against the Sinaloa and Jalisco cartels if you had that authorization use of military force, correct?

CHRISTOPHER WRAY:

I believe so. Although, now, you're getting a little bit out of my area of expertise.

MICHAEL WALTZ:

Would you welcome additional -- for example, offensive cyber from cybercom, would you welcome those additional resources? We know how to deconstruct cartels, terrorist organizations. We did it in the '90s in Colombia without a single American combat troop on the ground. And we can do it again. Now would you welcome those additional resources?

CHRISTOPHER WRAY:

Well, you'll never find an FBI director that won't welcome more tools in the fight.

MICHAEL WALTZ:

Fair enough. All right. Just switching -- that's good to hear. Just switching tacks. Director Haines, is ISIS and al-Qaeda's capability increasing in Afghanistan right now in terms of their capability to attack the West, attack US interests overseas, influence attacks in the United States, or even potentially attack the homeland?

Are they increasing?

AVRIL HAINES:

So, I wouldn't characterize them as increasing, although I would say certainly al-Qaida --

MICHAEL WALTZ:

-- They still have the intent.

AVRIL HAINES:

And yes, for ISIS in particular in Afghanistan, they still have the intent. But we can obviously go further in closed session on details.

MICHAEL WALTZ:

Is our collection capable -- have our collection capabilities since the summer of 2021 decreased in Afghanistan and in the surrounding region?

AVRIL HAINES:

Certainly with the removal of the US troops and presence in Afghanistan, absolutely. Our collection day to day has decreased, although I think again we can talk --

MICHAEL WALTZ:

-- We still have the groups that have the intent to attack us. I would -- I'm hearing --

AVRIL HAINES:

-- I think we can talk about what our collection posture is vis a vis those groups in Afghanistan in closed session and I think can give you some comfort on that issue.

WILLIAM BURNS:

I'm sorry, congressman. All I would add is of course it's true. You're right. Our capabilities are not the same as when we had a lot of presence on the ground. However, you know, as we've all promised you over the last couple of years, we work incredibly hard to try to ensure that we can still take action as the US government did against Ayman al-Zawahiri.

MICHAEL WALTZ:

I look forward to the closed session. However, you're going to have a hard time convincing me that managing sources by Zoom or remotely without being on the ground is anywhere near as effective. General Berrier, would you -- would the Chinese Communist Party -- would Beijing take note if we had an airbase a couple of hundred miles from their western border.

SCOTT BERRIER:

Yes, I believe they would.

MICHAEL WALTZ:

Twelve-thousand-foot runway that we could potentially stage strategic assets, a few hundred miles from their massive nuclear buildup.

SCOTT BERRIER:

Yes, I believe they would.

MICHAEL WALTZ:

Do you think -- I know this is a bit speculative. Do you think if the Chinese had a 12,000-foot runway a few hundred miles from the US border, they would give it up for free?

SCOTT BERRIER:
No.

MICHAEL WALTZ:
They would protect that asset, right? But we gave up Bagram Air Base. We no longer have access to that airbase. Is that correct?

SCOTT BERRIER:
That is correct.

MICHAEL WALTZ:
And the British government is now in negotiations to potentially -- we could potentially lose asset to Diego Garcia. Would that be significant?

SCOTT BERRIER:
That would be significant.

MICHAEL WALTZ:
Finally, Director Wray, can you -- you rightly sounded the alarm bell of opening a counterintelligence investigation every 12 hours with the director of MI-5. The National Science Foundation's had a 1,000 percent increase in referrals for grant theft, research theft. Yet you just answer me, I'm out of time.

MICHAEL WALTZ:
On shutting down the China initiative or rebranding it, renaming it, and at least from many people's perspective, diminishing it in priority. Just get that from the record.

CHRISTOPHER WRAY:
Well, I -- I can't speak to the Justice Department's initiative itself. All I can tell you is that, at the FBI, we're not taking our foot off the gas one iota on the threat posed by the Chinese Communist Party, including in the --

MICHAEL WALTZ:
But if we're not prosecuting -- we're not prosecuting with the same fervor, then that's an issue.

CHRISTOPHER WRAY:

Well, I think we're going to try to use every tool in the toolbox that we have. That'll include criminal prosecutions when we can do that. That'll include other things when we can do that.

MICHAEL WALTZ:

Thank you, Mr. Chairman.

MICHAEL TURNER:

Mr. Scott?

AUSTIN SCOTT:

Thank you. Mr. Chairman. Director Wray, I'm from Georgia. You've been there the last several years. Twenty years ago, if you looked at the list of groups that the SPLC would have said were hate groups, those groups would have been proud to have been named by them. And I think most Americans would have agreed with the list that they put out.

Today they put out lists with names like the American Family Association and the Alliance Defending Freedom. And yet, one of their attorneys was just recently charged in Atlanta with domestic terrorism. It -- it bothers me to see them cited as a source from your agency on who is and is not considered a domestic terrorist.

Can -- can you speak to the relationship between the FBI and -- and the influence the SPLC has? Is it just a list that you look at from time to time, or is there coordination?

CHRISTOPHER WRAY:

Well -- well, first off, just to be clear, I've considered Georgia my home since --

AUSTIN SCOTT:

Okay.

CHRISTOPHER WRAY:

Since I first got married, you know, back in 1989, so we have that in common. Second, as to the -- the product that you're referring to, the intelligence product, when I first saw it, and I said this yesterday, I was aghast. It was a --

AUSTIN SCOTT:

Okay.

CHRISTOPHER WRAY:

Single piece of an intelligence product by one field office. It did not meet our standards, and I had it immediately removed and withdrawn. And we've taken steps to make sure it doesn't happen again. And

one of the reasons I say that -- one of the ways in which I say that is the sourcing -- to your question, the sourcing didn't meet our standards.

AUSTIN SCOTT:

Thank you. You represent an agency that for years I held in the highest regard. I will tell you, I lost a lot of respect for the Justice Department and the FBI with what happened in a -- in a certain case in Valdosta where there was absolute evidence that a man and two kids had absolutely nothing to do with the death of another individual.

That man happened to be an FBI agent. And while he was -- he and his family were all cleared by state, local, and the FBI said nothing happened here, there was indisputable evidence. The US Attorney's office in Washington DC carried out a civil rights investigation for over two and a half years. And while that family was getting death threats repeatedly because of that investigation continuing to stay open, the US Attorney's office refused to release the absolute evidence of where all three individuals were.

What can be done to ensure that the -- that the US Attorney's office is held accountable when they take actions like that, that put Americans at risk, especially in this case, it was an FBI agent and his family?

CHRISTOPHER WRAY:

Well, I -- I confess I'm not familiar with the -- the specific case. In general, speaking just in general, when there are disciplinary violations by prosecutors, there's something called OPR, the Office of Professional Responsibility --

AUSTIN SCOTT:

I'm going to move on then. I'm going to -- I'm going to speak with you. We're going to get familiar with that case, because I think -- I think that the agents would like for you to probably be familiar with that case. China flew a spy balloon across the United States. And less than 15 days later, Ford Motor Company, one of America's most iconic brands, said they were going to team with CATL Technology to develop a multibillion dollar battery plant.

Director Haines, is it time for us to declassify a lot of the information that we have on China, their espionage and what they're doing to Americans and our industries, so that we can explain to corporate America that you -- you have to break your ties with communist China?

AVRIL HAINES:

Thank you, sir. We do actually and have been continuing to try to declassify as much information as we can on these issues so as to ensure the corporate America has everything that they need to protect themselves.

AUSTIN SCOTT:

The key to not going to war with China is for corporate America to understand they have the dual source or multi source and get out of there. With that, I yield the two seconds. And Director Wray, sorry I had to cut you off, but I'm on that clock.

MICHAEL TURNER:
Mr. Gallagher?

MICHAEL GALLAGHER:
Thank you. I apologize for being late. Director Wray, yesterday you expressed concern about the CCP's ability, through its ownership of ByteDance, to control narrative software data on TikTok. So long as ByteDance or another Chinese entity owns or maintains control of TikTok or its algorithm, would you maintain those concerns?

CHRISTOPHER WRAY:
Yes, it's the ownership of the CCP that fundamentally cuts across all those concerns.

MICHAEL GALLAGHER:
And specifically, ownership of the algorithm and control of the algorithm.

CHRISTOPHER WRAY:
Well, it's -- it's control of the algorithm. It's access to the data and it's the software's -- it's control of the software which allows access to the devices. So, you've got a -- a data collection issue, which could be used to conduct all kinds of data operations and traditional espionage. It's the algorithm, as you rightly pointed out, that enables them to conduct influence operations.

And as I said in response to an earlier question, that's particularly concerning because it's not at all clear we'd be able to detect that. And then third and finally, it's control of the software, which gives them access to millions of devices. And all you gotta do is look at the fact that the Chinese government has the biggest hacking program in the world, bigger than that of every other major nation combined, put that together with the fact that they have stolen more of Americans' personal and corporate data than every nation, big or small, combined, and you put that together with the risks that you and I are talking about, and to me, it highlights what a big concern this is.

MICHAEL GALLAGHER:
So, I guess the question is, for all of you, I'm just gonna go down, simply should we ban TikTok or force the sale to an American company?

CHRISTOPHER WRAY:
Well, I've expressed my concerns. I'm not sure how else the problem could be solved, but I've expressed my concerns, which are the ownership of the CCP.

MICHAEL GALLAGHER:
Is that a yes?

CHRISTOPHER WRAY:

Again, I don't speak to bans. That's not ultimately my -- that's a policy decision that's kind of beyond my --

MICHAEL GALLAGHER:

You all have a voice in the CFIUS process, correct?

CHRISTOPHER WRAY:

And we are absolutely -- I know that we are -- I think we all are expressing our assessments of the intelligence, the risks, the threats in the CFIUS process. But there's a -- the ultimate decision about that is beyond the scope of that.

MICHAEL GALLAGHER:

In the process, you haven't been asked yes or no yet, should we ban --

CHRISTOPHER WRAY:

Well, again, we submit our intelligence to the other participants, and then there's a committee that does its work.

MICHAEL GALLAGHER:

Director Burns, sorry to be obtuse. Should we ban or force the sale of TikTok to an American company?

CHRISTOPHER WRAY:

Well, all I'd say, Congressman, is I absolutely share the concerns that Director Wray has mentioned. But, you know, we're not in the business of, you know, making policy calls on bans or no bans. But I absolutely share the concerns, and we're not shy about expressing those concerns.

MICHAEL GALLAGHER:

So, in the CFIUS process, you don't get asked for a recommendation one way or the other?

CHRISTOPHER WRAY:

Well, speaking for the FBI, we -- we're asked to submit our intelligence assessment, but we're not asked for -- at least it's been my experience that we're not asked for a -- like a recommendation about what the ultimate decision should be.

AVRIL HAINES:

We --

MICHAEL GALLAGHER:
Director Haines, same question.

AVRIL HAINES:
Yeah. We do not provide a recommendation. Essentially, as Director Wray is indicating, what happens is our office pulls together the intelligence from the intelligence community that's relevant to any particular CFIUS transaction, and we provide that into the process essentially as, you know, grounds for policy discussion.

MICHAEL GALLAGHER:
Do you share Director Wray's concerns?

AVRIL HAINES:
I do share the concerns. I share the concerns of foreign entity owned social media platforms, other things that can, you know, be misused effectively. And we have a national OPSEC program is what we call it. The National Counterintelligence and Security Center runs this, and they have issued guidance essentially on these types of -- the use of these kinds of, you know, applications and platforms.

MICHAEL GALLAGHER:
General Nakasone, do you share Director Wray's concerns? Are you willing to answer the question, whether we should ban --

PAUL NAKASONE:
Certainly. Certainly. One third of -- one third of Americans get their news from TikTok every single day. One sixth of American youth say they're constantly on TikTok. That's a -- that's a loaded gun, Congressman. And as you know, we are executing for us the work to ensure that TikTok is not on government -- government applications and -- and IT.

MICHAEL GALLAGHER:
I'm out of time, but go for it.

SCOTT BERRIER:
I would -- I would just say we support the CFIUS process. And -- and as we brief decision makers on -- policymakers with the intelligence we have, our analysts are -- are in active and open dialog. If their opinions are asked, they will give those -- those opinions. I agree with everything that's been said here.

And I have a deputy director who has three teenagers. If -- if TikTok goes, she may not be able to go home.

MICHAEL GALLAGHER:

Thank you.

MICHAEL TURNER:

In closing, how -- pursuant to 707 Foreign Intelligence Surveillance Act 50 USC 1881A and F-AB-1 that you all provide to us annually a list of the -- the characterization of potential abuses of FISA. Director Wray, your answer to Congressman LaHood was that you have undertaken reforms internally and that you believe it would significantly reduce the overall abuses that we are all concerned about in the FBI. Anticipating that that might be your answer, we have a letter for you that we'll be presenting at the end of the hearing requesting that you go back and look at all of the reports that we have received that indicate those abuses and provide us, because it's going to be important to our working group, how those abuses that are identified would have been addressed under your new reforms so that we could find out what's remaining.

And if there's no objection, I'll -- I ask that this letter be entered into the record. No objection. Thank you all. You continue to show your professionalism and expertise in your answers, and we look forward to continue working with you. We'll be adjourned.

List of Panel Members and Witnesses

PANEL MEMBERS:

REP. MICHAEL TURNER (R-OHIO), CHAIRMAN

REP. BRAD WENSTRUP (R-OHIO)

REP. CHRIS STEWART (R-UTAH)

REP. RICK CRAWFORD (R-ARK.)

REP. ELISE STEFANIK (R-N.Y.)

REP. TRENT KELLY (R-MISS.)

REP. DARIN LAHOOD (R-ILL.)

REP. BRIAN FITZPATRICK (R-PA.)

REP. MIKE GALLAGHER (R-WIS.)

REP. AUSTIN SCOTT (R-GA.)

REP. FRENCH HILL (R-ARK.)

REP. DAN CRENSHAW (R-TEXAS)

REP. MICHAEL WALTZ (R-FLA.)

REP. MIKE GARCIA (R-CALIF.)

REP. JIM HIMES (D-CONN.), RANKING MEMBER

REP. ANDRE CARSON (D-IND.)

REP. JOAQUIN CASTRO (D-TEXAS)

REP. RAJA KRISHNAMOORTHY (D-ILL.)

REP. JASON CROW (D-COLO.)

REP. AMI BERA (D-CALIF.)

REP. STACEY PLASKETT (D-V.I.)

REP. JOSH GOTTHEIMER (D-N.J.)

REP. JIMMY GOMEZ (D-CALIF.)

REP. CHRISSY HOULAHAN (D-PA.)

REP. ABIGAIL SPANBERGER (D-VA.)

WITNESSES:

DEFENSE INTELLIGENCE AGENCY DIRECTOR SCOTT D. BERRIER

CENTRAL INTELLIGENCE AGENCY DIRECTOR WILLIAM J. BURNS

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE DIRECTOR AVRIL HAINES

NATIONAL SECURITY AGENCY DIRECTOR PAUL NAKASONE

FEDERAL BUREAU OF INVESTIGATION DIRECTOR CHRISTOPHER WRAY

1201 Pennsylvania Ave NW, 6th floor · Washington, D.C. 20004 · 202-793-5300
About CQ Help Privacy Policy Masthead Terms & Conditions

DEFENDANTS' EXHIBIT 139:

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

The State of Louisiana,
et al.,

Plaintiffs,

v.

**President Joseph R. Biden, Jr., in his
official capacity as President of the United
States of America,**
et al.,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF JASMINE ROBINSON

1. My name is Jasmine Robinson. I am a paralegal employed by the United States Department of Justice. I am over eighteen years of age and competent to testify to the matters discussed herein.

2. On April 20, 2023, I went onto LinkedIn and found an active LinkedIn account for Plaintiff Martin Kulldorff. That account can be found here:

<https://www.linkedin.com/in/martin-kulldorff-8a31a775>. See Ex. A.

3. On April 20, 2023, I went onto Facebook and found an active Facebook account for Plaintiff Jill Hines. Her active Facebook account can be found here:

<https://www.facebook.com/jillhines4freedom/>. See Ex. B.

4. On April 20, 2023, I went onto Twitter and found an active Twitter account for the Gateway Pundit, a company founded, owned and operated by Plaintiff Jim Hoft. That account can be found here: <https://twitter.com/gatewaypundit>. See Ex. C.

5. On April 20, 2023, I went onto Twitter and found an active Twitter account for Plaintiff Daniel Kotzin. That account can be found here: https://twitter.com/danielkotzin?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor. *See* Ex. D.

6. On April 20, 2023, I went onto Twitter and found an active Twitter account of Plaintiff Amanda (“A.J.”) Kitchen. Her active Twitter account can be found here: https://twitter.com/AJKayWriter?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor. *See* Ex. E.

7. On April 20, 2023, I went onto Twitter and found an active Twitter account for Michael P. Senger, an individual who submitted a declaration in this matter. His active Twitter account can be found here: https://twitter.com/MichaelPSenger?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor. *See* Ex. F.

8. On April 20, 2023, I went onto Facebook and found an active Facebook account HFL Group. The HFL Group’s active Facebook can be found here: <https://www.facebook.com/groups/1240524952709254/>. *See* Ex. G.

9. Attached hereto as Exhibit H is an article from David Klepper and Heather Hollingsworth from AP News entitled “Misinformation at public forums vexes local boards, big tech.” (Aug. 16, 2021).

10. On April 20, 2023, I went onto Twitter and found an active Twitter account for Mark Changizi. Mr. Changizi’s Twitter account may be found here: <https://twitter.com/MarkChangizi>. *See* Ex. I.

11. On May 1, 2023, I went onto Twitter and found an active Twitter account for Dr. Robert Malone. Dr. Malone’s Twitter account may be found here:

<https://twitter.com/RWMaloneMD>. See Ex. J.

I swear or affirm, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge.

Dated: May 1, 2023

Signed:

JASMINE
ROBINSON

Digitally signed by
JASMINE ROBINSON
Date: 2023.05.01
14:26:59 -04'00'

Jasmine Robinson



EXHIBIT A



Martin Kulldorff

Biostatistician and epidemiologist. Author of the Great Barrington Declaration.

Talks about #covid19, #pandemic, #vaccines, #publichealth, and #epidemiology

-  Harvard Medical School
-  Cornell University

United States · [Contact info](#)

14,990 followers 500+ connections

Follow

[Message](#)

[More](#)

Featured

Post

[#covid19](#) [#socialdistancing](#) [#coronavirus](#) [#herdimmunity](#) [#epidemiology](#) [#t](#)

COVID 19 Counter Measures Should be Age Specific

Martin Kulldorff on LinkedIn · 6 min read

   406

Activity

14,990 followers

[+ Follow](#)

Martin Kulldorff posted this · 1w

Truth seems to be prevailing, but ... we have a crisis of trust that threatens the credibility of all future health guidance. The WHO does not deserve public trust, yet...



W.H.O. Do You Trust?

newsweek.com · 6 min read

   357

46 comments

Martin Kulldorff posted this · 1w


On Friday March 10th, 2023, Silicon Valley Bank died of Covid ... in all the discussion of the current bank runs, the pivotal role of lockdowns in priming the crisis remains overlooked. ...

   198

35 comments

Martin Kulldorff posted this · 3w

The American people deserve a bipartisan, scientifically minded COVID-19 commission so the public-health disaster of the past three years is not r ...show more



Why America needs a COVID truth commission
nypost.com • 4 min read

544 36 comments

Martin Kulldorff posted this • 1mo

Public health crashed. It is now imperative to form a commission to conduct a thorough and open minded COVID inquiry [show more](#)

We Need a COVID Commission
newsweek.com • 3 min read


853 69 comments

Show all activity →

About

I develop statistical and epidemiological methods for the detection and monitoring of disease outbreaks and for drug and vaccine safety surveillance. In collaboration with others, I use those methods in a wide variety of settings. On LinkedIn, I provide updates on the COVID-19 pandemic.


Experience




Harvard Medical School
12 yrs 3 mos
Boston, MA, United States

Professor
2015 - Present 8 yrs 3 mos
Department of Medicine (leave of absence since October 2021)


Professor
2011 - 2015 4 yrs
Department of Population Medicine.




Professor of Medicine
Brigham and Women's Hospital
2015 - 2021 6 yrs
Boston, Massachusetts, United States
Division of Pharmacoepidemiology and Pharmacoeconomics



Associate Professor
Harvard Medical School
2003 - 2010 7 yrs
Boston, MA, United States
Department of Population Medicine (formerly Department of Ambulatory Care and Prevention)




Associate Professor
University of Connecticut
1998 - 2003 5 yrs
Farmington and Storrs, CT, United States
Department of Community Medicine, and, Adjunct Associate Professor, Department of Statistics



Scientist
National Cancer Institute (NCI)
1995 - 1998 3 yrs
Bethesda, MD, United States
Biometry Branch, Division of Cancer Prevention


Show all 10 experiences →



Cornell University

Doctor of Philosophy (PhD), Operations Research and Industrial Engineering

1984 - 1989



Umeå University


Bachelor of Science (BSc), Mathematical Statistics


1981 - 1984

Skills


Biostatistics

Endorsed by Lingling Li and 4 others who are highly skilled at this


 Endorsed by 2 colleagues at Harvard Medical School

 51 endorsements

Scan Statistics

 10 endorsements

Spatial Statistics

 8 endorsements

Show all 27 skills →

Recommendations

Received

Given

Nothing to see for now

Recommendations that Martin receives will appear here.

Publications

Drug safety data mining with a tree-based scan statistic

Pharmacoepidemiology and Drug Safety Jan 1, 2013

Show publication ↗

Kulldorff M, Dashevsky I, Avery TR, Chan KA, Davis RL, Graham D, Platt R, Andrade SE, Boudreau D, Gunter MJ, Herrinton LJ, Pawloski P, Raebel MA, Roblin D, Brown JS.

A maximized sequential probability ratio test for drug and vaccine safety surveillance

Sequential Analysis Jan 1, 2011

Show publication ↗

Kulldorff M, Davis RL, Kolczak M, Lewis E, Lieu T, Platt R.

https://www.linkedin.com/in/martin-kulldorff-8a31a775/

3/6

Tests for spatial randomness adjusting for an inhomogeneity: A general framework.

Journal of the American Statistical Association Jan 1, 2006

Show publication ↗

Kulldorff M.

Show all 6 publications →

Languages

Danish

Professional working proficiency

English

Full professional proficiency

German

Elementary proficiency

Show all 7 languages →

Causes

Education • Health • Human Rights • Science and Technology

Interests

Top Voices

Companies

Groups

Newsletters

Schools



David L. Katz, MD, MPH [in](#)

CEO, DietID; President, True Health Initiative. Founding Director, Yale-Griffin PRC (1998-2019). Health Journalist. COVID Curmudgeon

902,065 followers

+ Follow



People also viewed



Stefanos Kales 3rd+

Professor of Medicine at Harvard Medical School

Message



Bret Weinstein 3rd+

Former Evolutionary Biologist and Professor at The Evergreen State College.

Message



Vinay Prasad 3rd+
Professor of Epidemiology and Biostatistics; Doctor; Writer

Message



Christine Stabell Benn 3rd+
Professor, Global Health @SDU. Studying the overall health effects of vaccines in Guinea-Bissau and Denmark, discovering that they have...

Message

Del Bigtree 3rd+
--

Connect

Show more

People you may know



Matt Galvin
Counsel, Compliance & Data Analytics at U.S. Department of Justice

Connect



Jessica H. Kim
Chief of Staff & Counselor (Acting), Criminal Division, U.S. Department of Justice

Connect



Jordan Esteban
Trial Attorney at U.S. Department of Justice

Connect

Ali Gadelhak
Trial Attorney at U.S. Department of Justice

Connect

Julia Birnbach
DOJ Paralegal

Connect

Show more

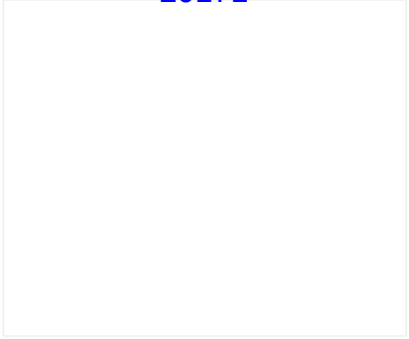


EXHIBIT B

facebook

Log In



Jill Hines for Republican State Central Committee

599 likes • 615 followers

Posts About Photos Videos ...

Intro

My hope is to raise awareness in Louisiana for the need to protect our God-given right to make healt

i Page · Community

✉ reopenla@gmail.com

Connect with Jill Hines for Republican State Central Committ...

Log In or Create new account

facebook

Log In

  70

24  10 

 Like

 Comment

Most relevant 



Heather Welsh

This is awesome you will be amazing at this...

1y

[View 10 more comments](#)

Other posts



Jill Hines for Republican State Central Committee

June 10 2021 

Update on HB498 🙌🙌



Connect with Jill Hines for Republican State Central Committ...

Log In

or

Create new account



Log In

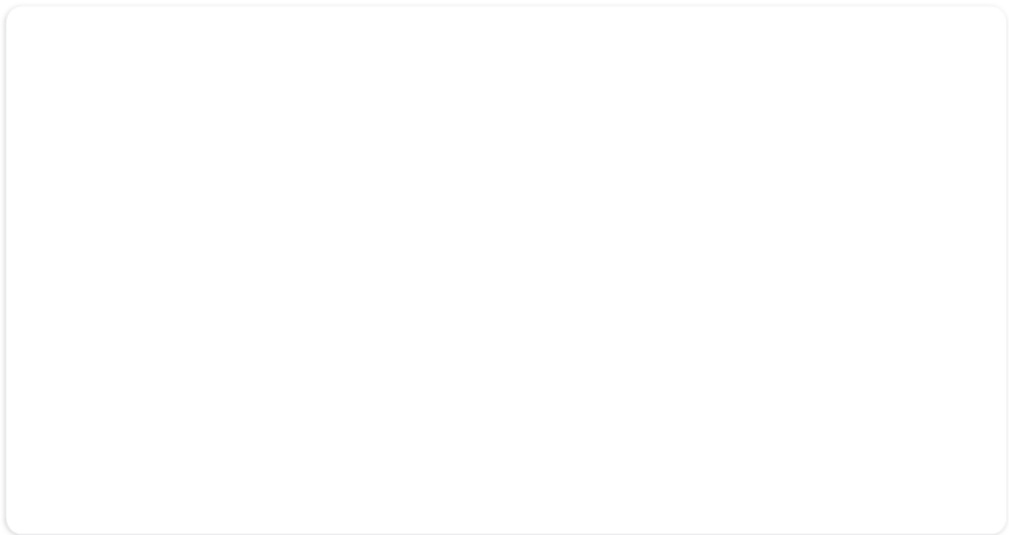
Rep Edmonston had to take the bill to conference committee after
Senator Stewa... See more



Like



Comment



Connect with Jill Hines for Republican State Central Committ...

Log In

or

Create new account

EXHIBIT C




Explore

⚙ Settings

🔍 Search Twitter

New to Twitter?

Sign up now to get your own pen

 Sign up with G

 Sign up with A

Create accou

By signing up, you agree to the T
Privacy Po icy, inc uding Cookie

You might like

kanekoa.substack
@KanekoaTheGrea

James O'Keefe ✓
@JamesOKeefeIII

Tracy Beanz ✓
@tracybeanz

[how mo e](#)

What's happening

NBA Last night
Suns at Lakers

Jungkook · Trending
jungkook
241K Tweets

Trending in United States
SAY WHAT
236K Tweets

Sports · Trending
Demarco Murray

Trending in United States
TikTok
Trending with [ByteDance](#)

[how mo e](#)

e ms of Se v ce P vacy Po c
Access b y Ads nfo Mo e +
© 202 Tw e nc

The Gateway Pundit ✓

@gatewaypundit

Follow

The Gateway Pundit ✓

118.6K Tweets

Follow

[thegatewaypundit.com](#) 📅 Joined January 2009

1,638 Following 501.6K Followers

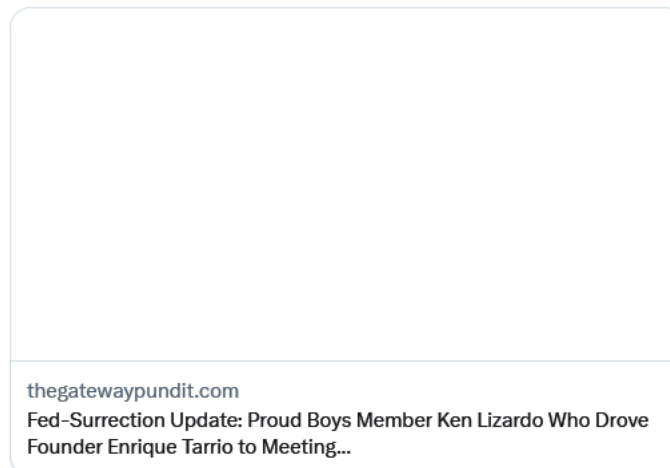
Tweets

Replies

Media

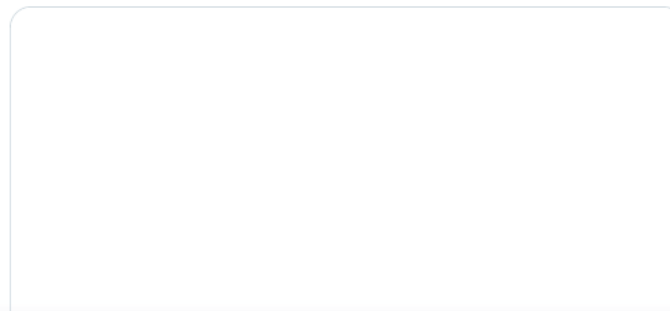
Likes

The Gateway Pundit ✓ @gatewaypundit · 11m
Fed-Surrection Update: Proud Boys Member Ken Lizardo Who Drove
Founder Enrique Tarrio to Meeting with Oath Keepers Founder on Jan. 5th
Was an FB Operative



🗨 4 🔄 69 ❤ 89 📊 3,253 📤


The Gateway Pundit ✓ @gatewaypundit · 21m
B G DEVELOPMENT: President Trump Repub lishes Stormy Danie s 2018
Letter Denying Ever Having a Re ationship with Dona d Trump



Don't miss what's happening

Peop e on Twitter are the first to know.

Log in S



Explore

⚙ Settings

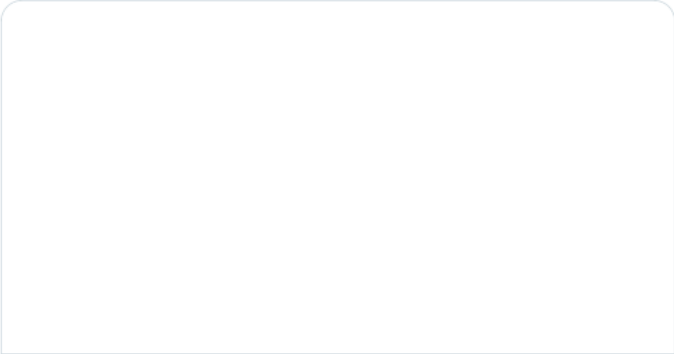
THE GATEWAY PUNDIT (@gatewaypundit) / Twitter

BIG DEVELOPMENT: FIVE MORE Trump Repub Shes Stormy Danes 2018 Letter Denying Ever Having a...

9 7 278 589

The Gateway Pundit @gatewaypundit · 51m

Joe Biden: “ Like Babies Better Than Peop e” (V DEO)

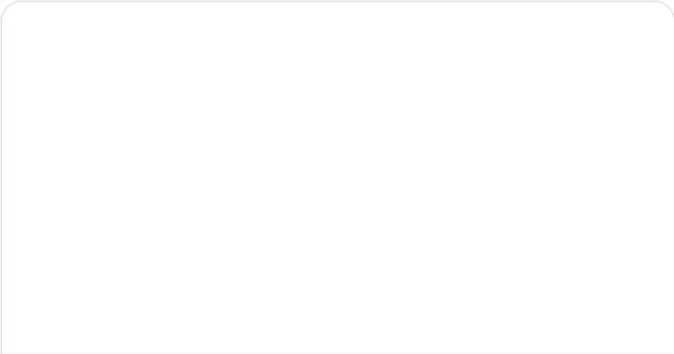


thegatewaypundit.com
Joe Biden: Like Babies Better Than Peop e (V DEO)

26 9 2 K


The Gateway Pundit @gatewaypundit · 56m

Father of Park and Schoo Shooting Victim Arrested After Disrupting Congressiona Hearing (Video)



thegatewaypundit.com
Father of Park and Schoo Shooting Victim Arrested After Disrupting Congressiona Hearing (Video)


9 25 707


 The Gateway Pund t Retweeted

Julie Kelly @julie_kelly2 · 6h

Lizardo actua y picked up Tarrio from jai then drove him to the garage for infamous meet-up with Stewart Rhodes (Oath Keepers) the day before Jan 6.

One wou d think his testimony wou d be crucia for the jury to hear. But they won t thanks to Judge Ke y






Explore

Settings

5 22 59 22.6K

how th s thread


The Gateway Pundit  @gateway pundit · 1h

C U V NT RV W Mothe of Peacefu 6 P sone "QAnon haman" a e Chans ey ays He W e Re eased om P son "Rea y oon "

thegateway pundit com

C U V NT RV W Mothe of Peacefu 6 P sone QAnon haman a e Chans ey ays He W e

25 194 522 10.5K

The Gateway Pundit  @gatewaypundit · 1h

Ray Epps Sends to Letter to Tucker Carlson Demanding Retraction by March 31 #FedEpps

thegatewaypundit.com

Ray Epps Sends to Letter to Tucker Carlson Demanding Retraction by March 31 #FedEpps

587 796 1,336 61.1K



Explore

⚙ Settings

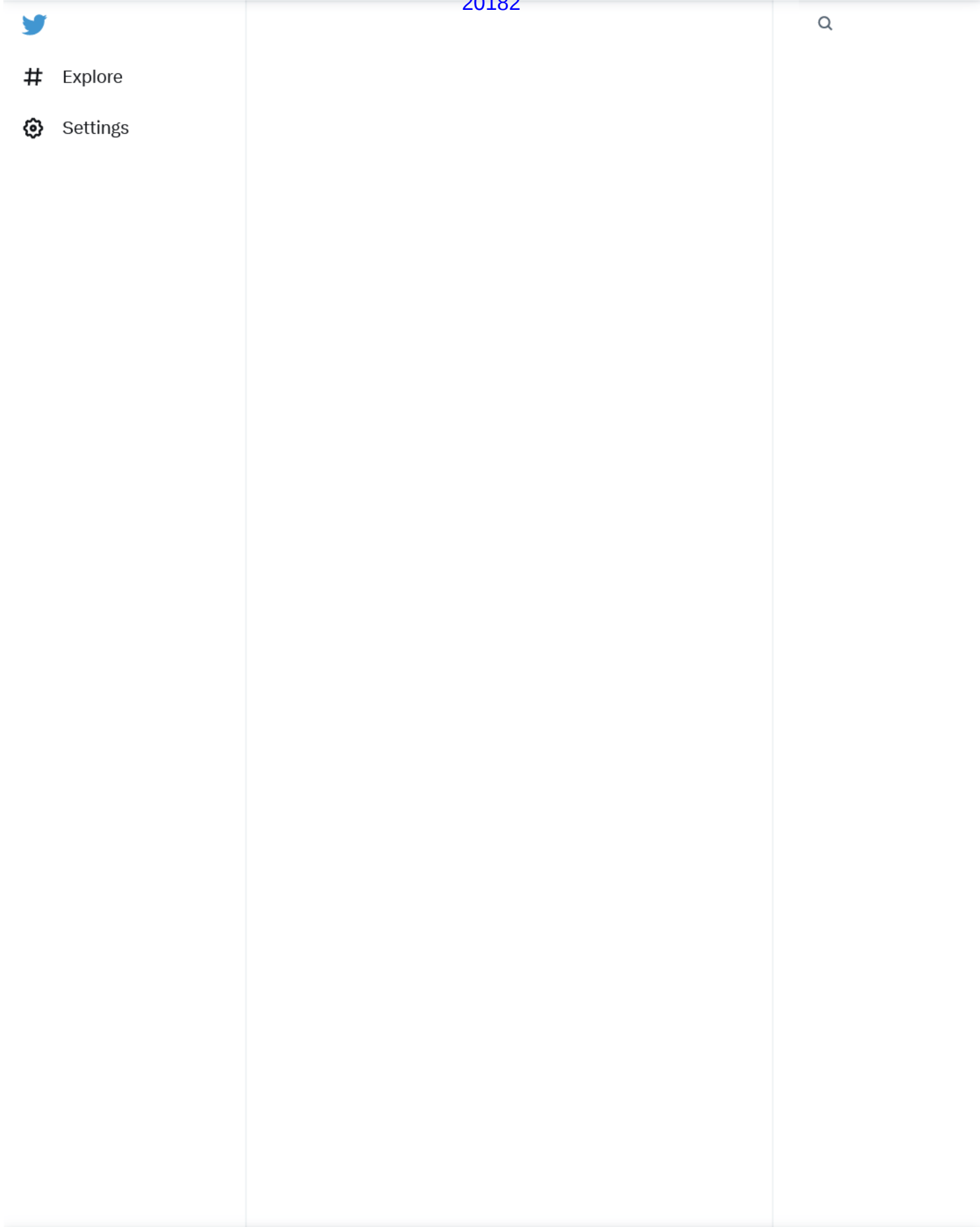


Don't miss what's happening

People on Twitter are the first to know.

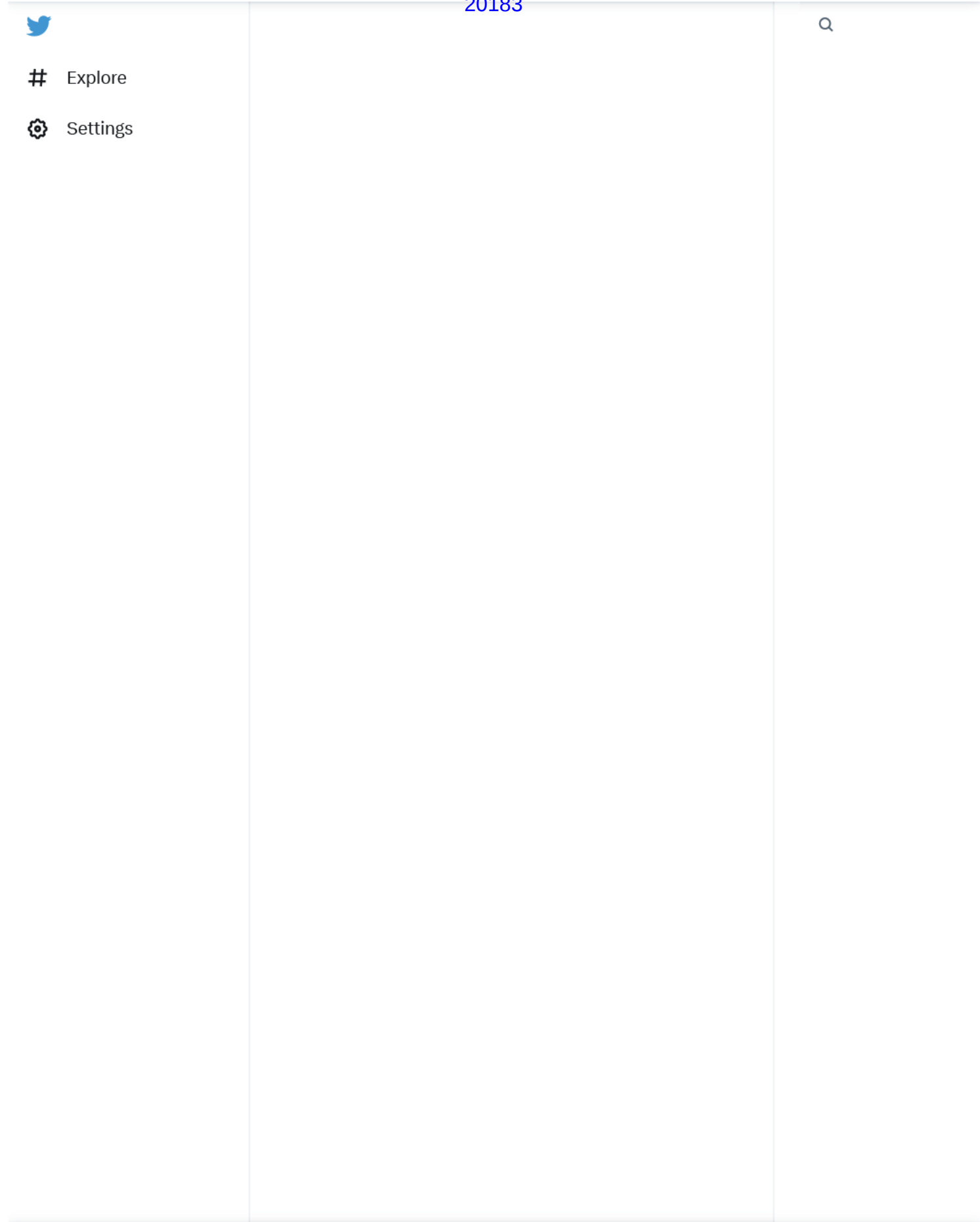
Log in

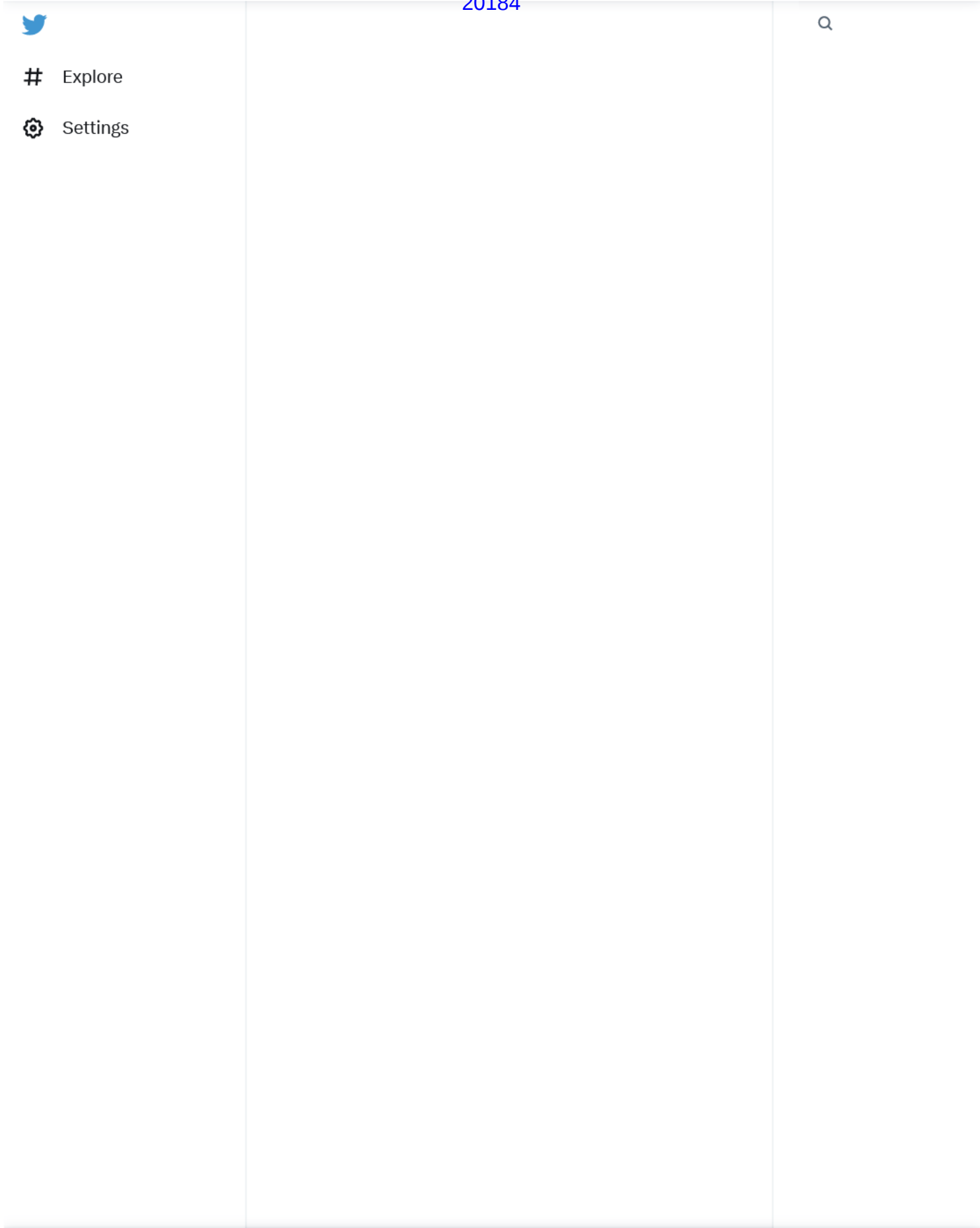
S



Don't miss what's happening
People on Twitter are the first to know.

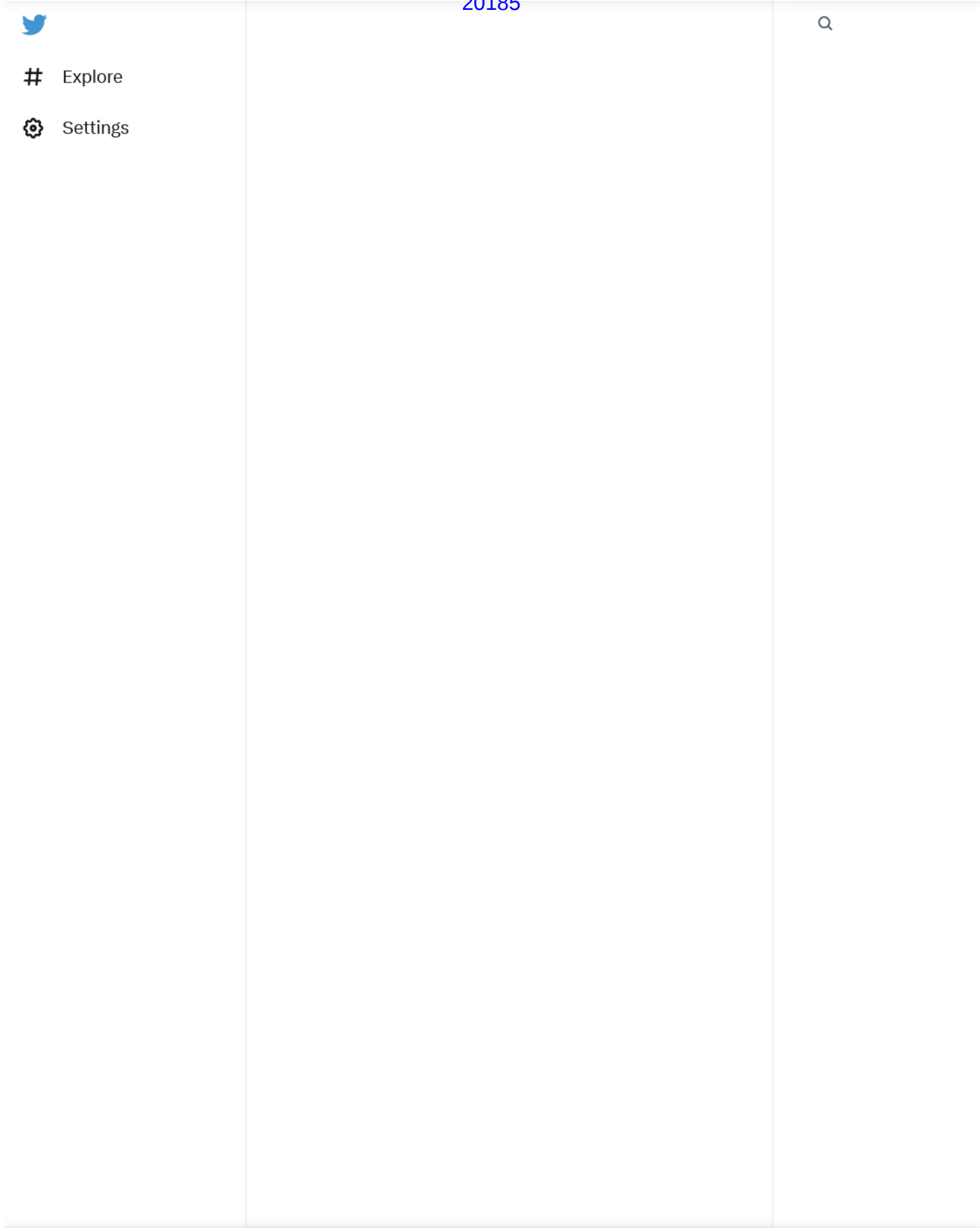
Log in S





Don't miss what's happening
People on Twitter are the first to know.

Log in S



Don't miss what's happening
People on Twitter are the first to know.

Log in **S**



Explore

⚙ Settings



Don't miss what's happening

People on Twitter are the first to know.

Log in

S

EXHIBIT D

Explore

Settings

←

Daniel Kotzin

11.2K Tweets

MARK CHANGIZI,
MICHAEL P. SENER,
DANIEL KOTZIN,

Plaintiffs,

v.

DEPARTMENT OF HEALTH AND
SERVICES;
MURTHY, United States
Attorney General, in his
official capacity

Civil Action No.: 2:22-cv-01776

Motion for Preliminary Injunction

Follow

Daniel Kotzin

@danielkotzin

Stay-at-home dad. Human rights activist. My freedom protects you; your freedom protects me.

Denver, CO

[danielkotzin.substack.com](#)

Joined Apr 2013

291 following 40.2K followers

Tweets

Replies

Media

Likes

Daniel Kotzin

@danielkotzin · Jan 17, 2021

am not a Covid denier. I am a lockdown denier.

deny the right of the government to lockdown healthy people.

deny cuffs, and taser, and unnecessary closures. deny shuttered churches.

deny dying alone. deny custody to children. deny forced family separation.

688 replies 7 retweets 25.7K likes

Daniel Kotzin

@danielkotzin · 6h

The Denver Board of Ed's misguided removal of police officers from schools has had predictable tragic consequences.

But there is no apology. No remorse. And no mention of the 17-year-old high school student who killed himself yesterday and for whose death they are responsible.

Auon'tai M Anderson

@Auon'tai Anderson · 7h

We are devastated to learn that once again, a high school has experienced gun violence. We first want to extend our support and care to the two school leaders who were shot. We also share concern for the students, staff, and families of the student who died once again.

[how more](#)

DENVER PUBLIC SCHOOLS

Board of Education

STATEMENT

Search Twitter

New to Twitter?

Sign up now to get your own profile.

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Twitter Privacy Policy, including Cookies.

You might like

Brian Tyson, MD

@btysonmd

Abir Ballan

@abirballan

Dr. Lynn Fynn-der

@Fynnnderella1

[how more](#)

What's happening

NBA Last night
Suns at Lakers

Trending in United States
TikTok
Trending with ByteDance

Jungkook · Trending
jungkook
364K Tweets

Trending in United States
Vertigo
3,938 Tweets

Sports · Trending
Jason Whitlock
3,268 Tweets

[how more](#)

Terms of Service

Privacy Policy

Accessibility

Ad info

More

© 2021 Twitter, Inc.

Don't miss what's happening

People on Twitter are the first to know.

Log in

S

https://twitter.com/danielkotzin?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor 1/8



Explore

Settings

**Daniel Kotzin**  @danielkotzin · 7h

American public schools are supposed to educate children, not indoctrinate them.

School Boards are supposed to serve communities, not political agendas.

 2  2  31  1,232 

**Daniel Kotzin**  @danielkotzin · 7h

For those wondering why Denver's School Board decided a couple of years ago not to allow police in schools, it's because the police are supposedly racist

The evidence? 1 in 7 students in Denver were black, but 1 in 4 of the students arrested or ticketed at school were black.

 1   9  1,040 

**Daniel Kotzin**  @danielkotzin · 20h

In the wake of today's shooting, @MayorHancock called removing police from Denver Public Schools a "mistake."

This tragic mistake was made by the Denver Board of Education, and it typifies their disregard for the well-being of students, teachers, and staff.

 7  30  132  11.4K 

**Daniel Kotzin**  @danielkotzin · Mar 22

Today in Denver, 2 faculty members were shot while checking a high school student for weapons. That's a job for police, not teachers. But there are no police officers allowed in Denver Public Schools because the School Board recently voted to remove them.



[cnn.com](https://www.cnn.com)
2 adult victims injured in shooting at Denver high school CNN
Denver Police said in a Twitter post that they are responding to a shooting at East High School in Denver, Colorado.

 16  53  131  7,074 

**Daniel Kotzin**  @danielkotzin · Mar 21

Remember that they said that anyone who refuses the covid "vaccines" is selfish and stupid.

They made us submit in order to keep our jobs, or attend university, or go to camp.

They would not let us eat at restaurants.

They said that the pandemic is our fault.

Do not forget!

 50  228  1,068  78.8K 

Don't miss what's happening
People on Twitter are the first to know.

Log in

S

Explore

Settings

Search

How can anyone believe that the “vaccines” have a positive impact on infection transmission after looking at this graph?

Cases

7-day rolling average. Due to limited testing, the number of confirmed cases is lower than the true number of infections.

LINEAR

LOG

+ Add country

Aug 6, 2021

United States 97,880.86

5

5

46

2,303

Don't miss what's happening

People on Twitter are the first to know.

Log in

S

https://twitter.com/danielkotzin?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

3/8



Explore

⚙ Settings

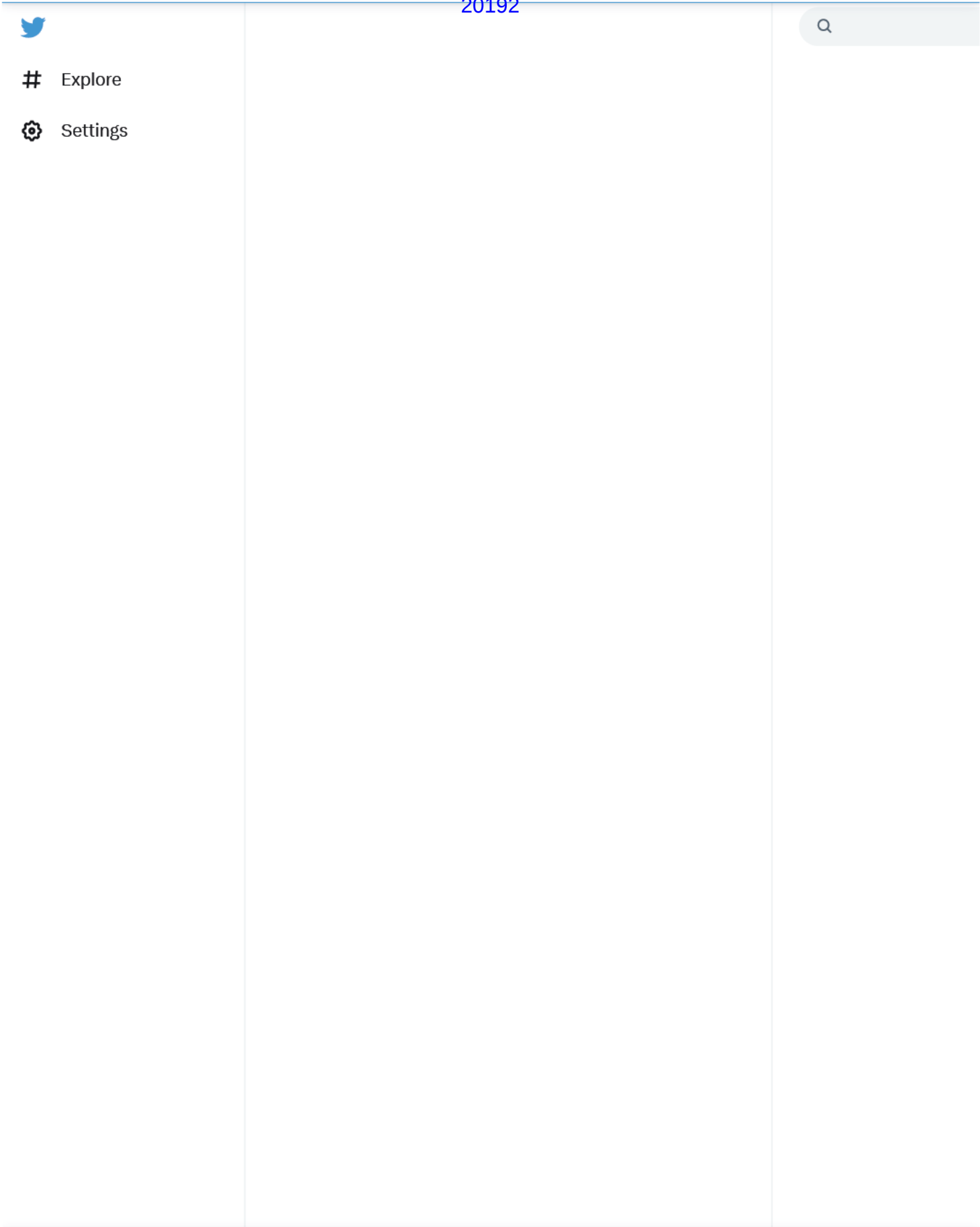


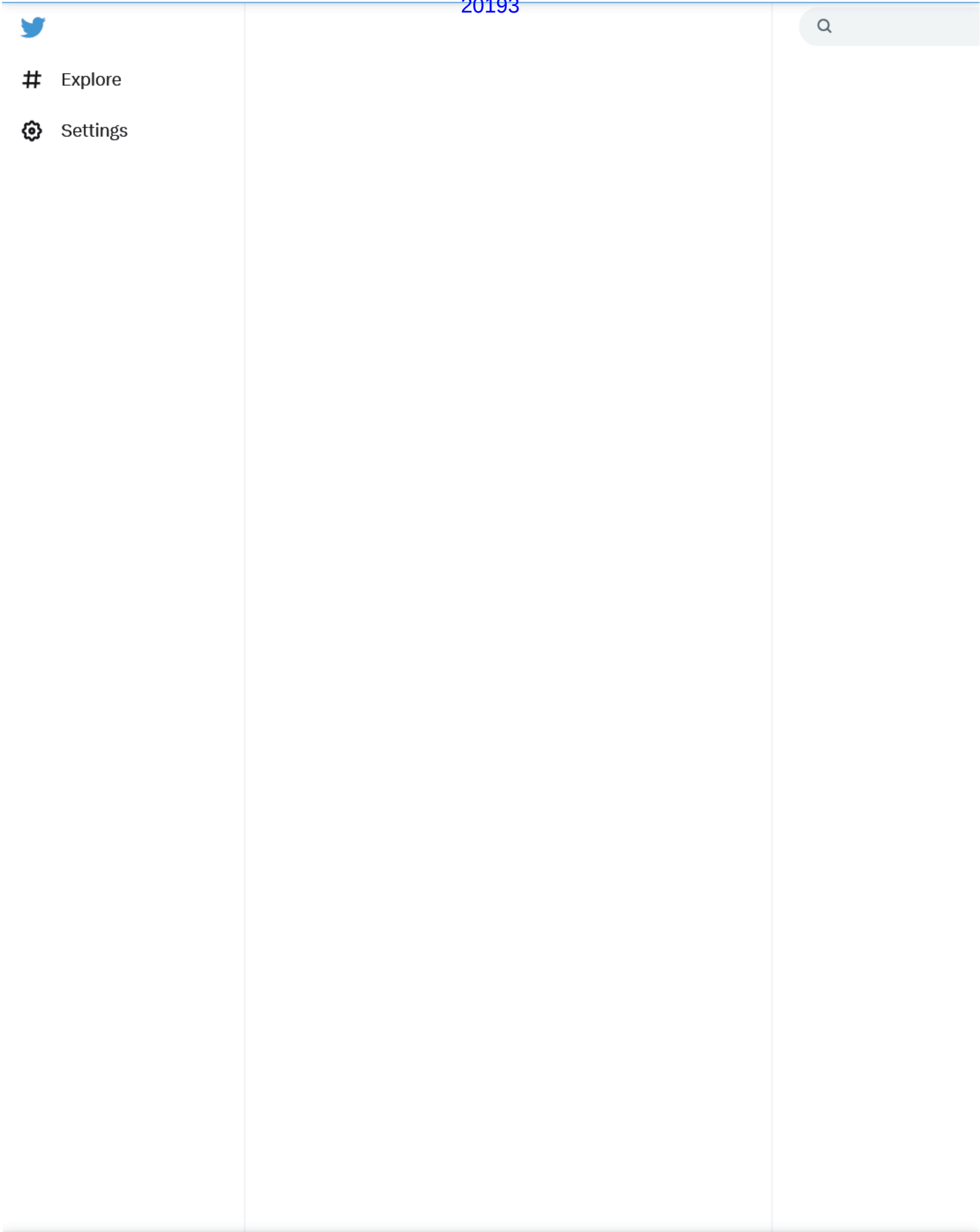
Don't miss what's happening

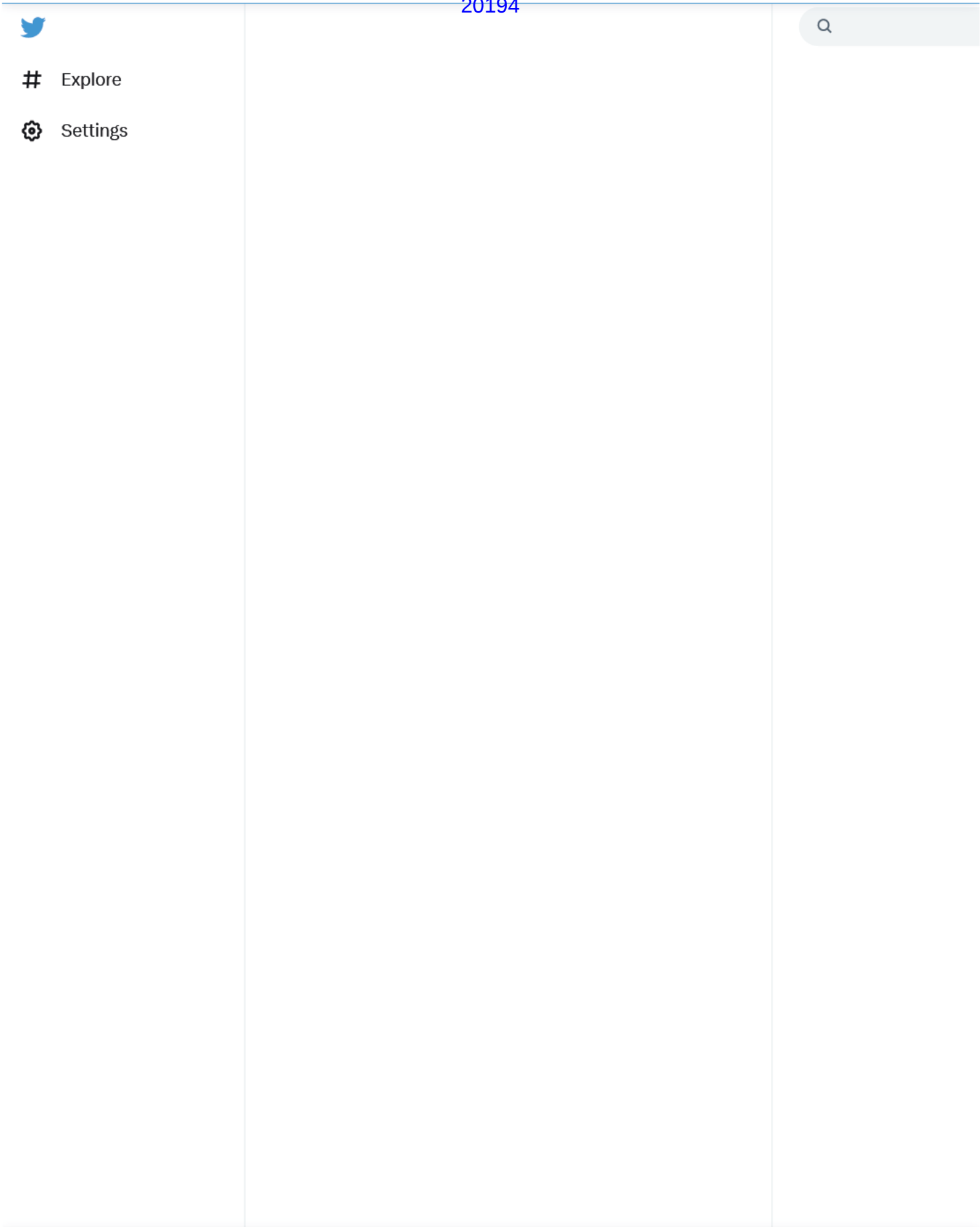
People on Twitter are the first to know.

Log in

S







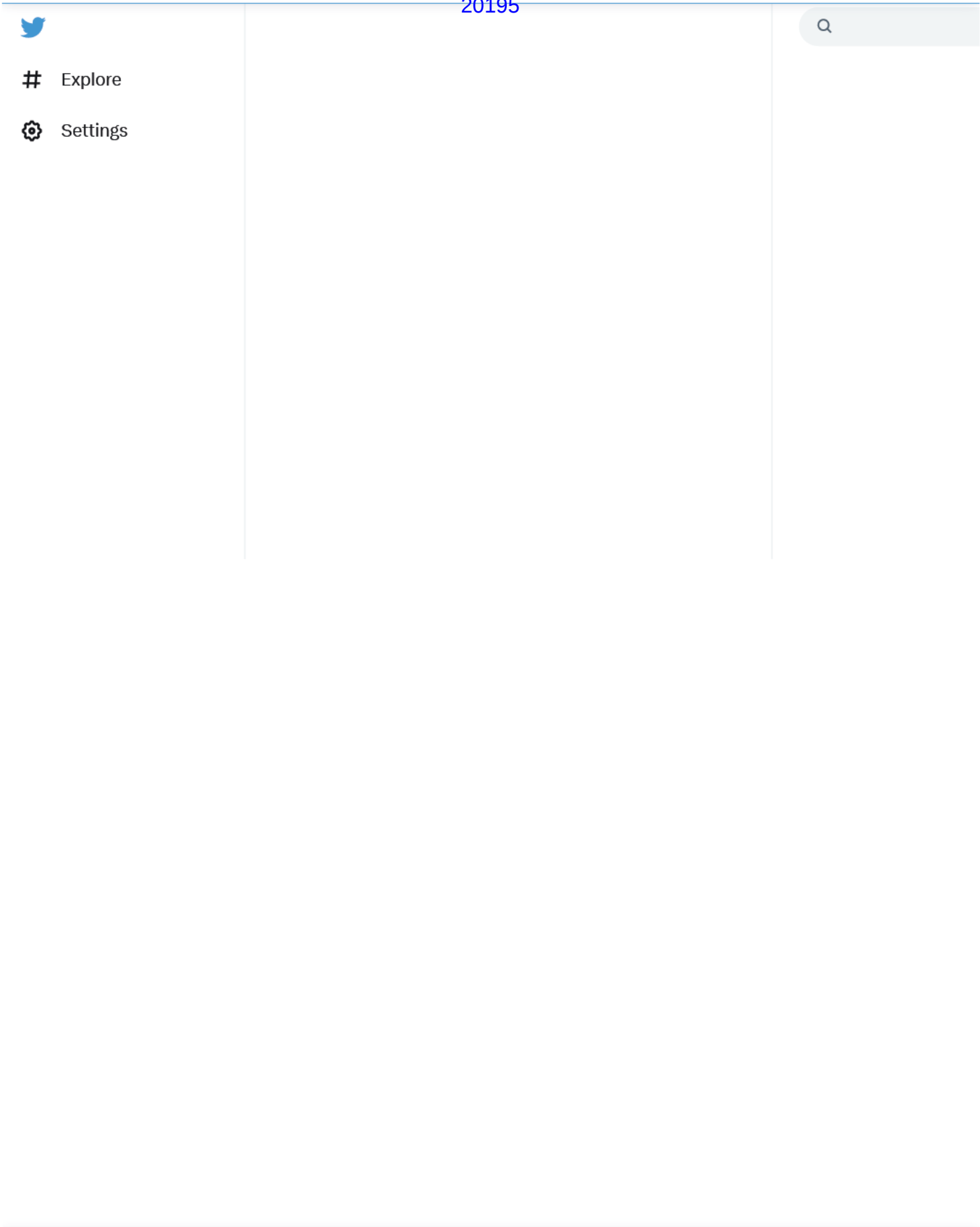




EXHIBIT E



Explore


Settings



This critique seems funny to me. The point is not to calculate the proportion of erroneous data to accurate data.

It's to characterize the nature of the errors.

And the directional near-uniformity of said errors point to systematic bias v. randomness (like the typo DM cited.)


David Meyer @da_meye · 3h

Replying to @KelleyKga and @AJKayWriter
 To put the number of errors you identified in context, can you estimate the total number of numerical/statistical statements @CDCgov made during 2021 present? After all, we all make mistakes, e.g., the table in your article contains an entry for Aug 20, 2023


2

1

4

1,407

Show this thread


Kelley K @KelleyKga · 5h

Three years ago when I started tracking Covid data in Georgia, I never imagined I'd end up co-authoring a paper on basic mathematical errors the CDC made during the pandemic. Most of the errors exaggerate the risk to children. [papers.ssrn.com/sol3/papers.cfm...](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4688883)


89

489

1,375

137.7K

Show this thread


AJ Kay @AJKayWriter · 5h

OW, essentially all of the CDC's errors point in the same direction: overstatement.

Overstatement → inflated public perception of severity.

Inflated perception of severity → panic-driven policies.

Panic-driven policies → harm.

Ergo:

CDC → Harm


2

3


30

1,660

Show this thread


AJ Kay @AJKayWriter · 5h

The relevance in quantifying what's already apparent, e.g. this article where I, @KelleyKga, @TracyBethHoeg, Alyson Haslam & @VPasadm MPH found that the CDC's data and related messaging on Covid was overloaded & systematically biased resulting in overstated risks & severity


Benjamin Ryan @benryanwriter · 5h

In a new paper, @TracyBethHoeg, @KelleyKga and @vkprasad ab chronic the statistical and numerical errors that the CDC made during the Covid-19 pandemic. In 80% of cases, the CDC exaggerated the severity of the pandemic. [papers.ssrn.com/sol3/papers.cfm...](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4688883)

Show this thread

Abstract
 Background: The Centers for Disease Control and Prevention (CDC) has been a major source of information during the COVID-19 pandemic, guiding policies and practices in many aspects of life. As such, it is imperative that the information be free of errors, or, if errors are made, that they are corrected quickly.


Don't miss what's happening
People on Twitter are the first to know.

Log in

S

https://twitter.com/AJKayWriter?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor

2/8



Explore

Settings

Results: We documented 25 instances when the CDC reported statistical or numerical errors. Twenty (80%) of these instances exaggerated the severity of the COVID-19 situation, 3 (12%) instances simultaneously exaggerated and downplayed the severity of the situation, one error was neutral, and one error exaggerated COVID-19 vaccine risks. The CDC was notified about the errors in 16 (64%) instances, and later corrected the errors, at least partially, in 13 (52%) instances.

Conclusion: A basic prerequisite for making informed policy decisions is accurate and reliable statistics, even during times of uncertainty. Our investigation revealed 25 instances of numerical or statistical errors made by the CDC. Our investigation suggests 1) the need for greater diligence in data collection and reporting, and 2) that the federal entity responsible for reporting health statistics should be firewalled from the entity setting policy due to concerns of real or perceived systematic bias in errors.

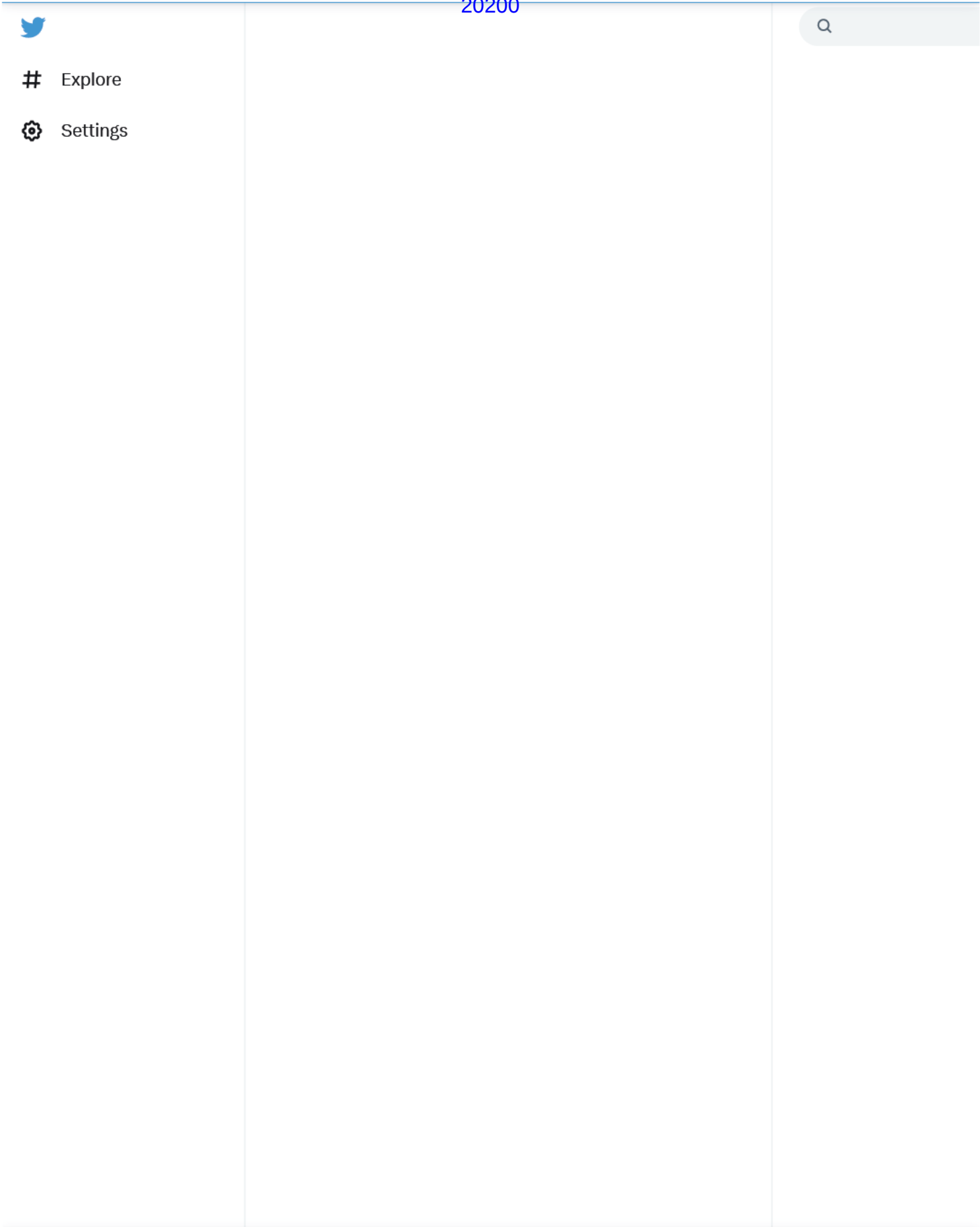
1

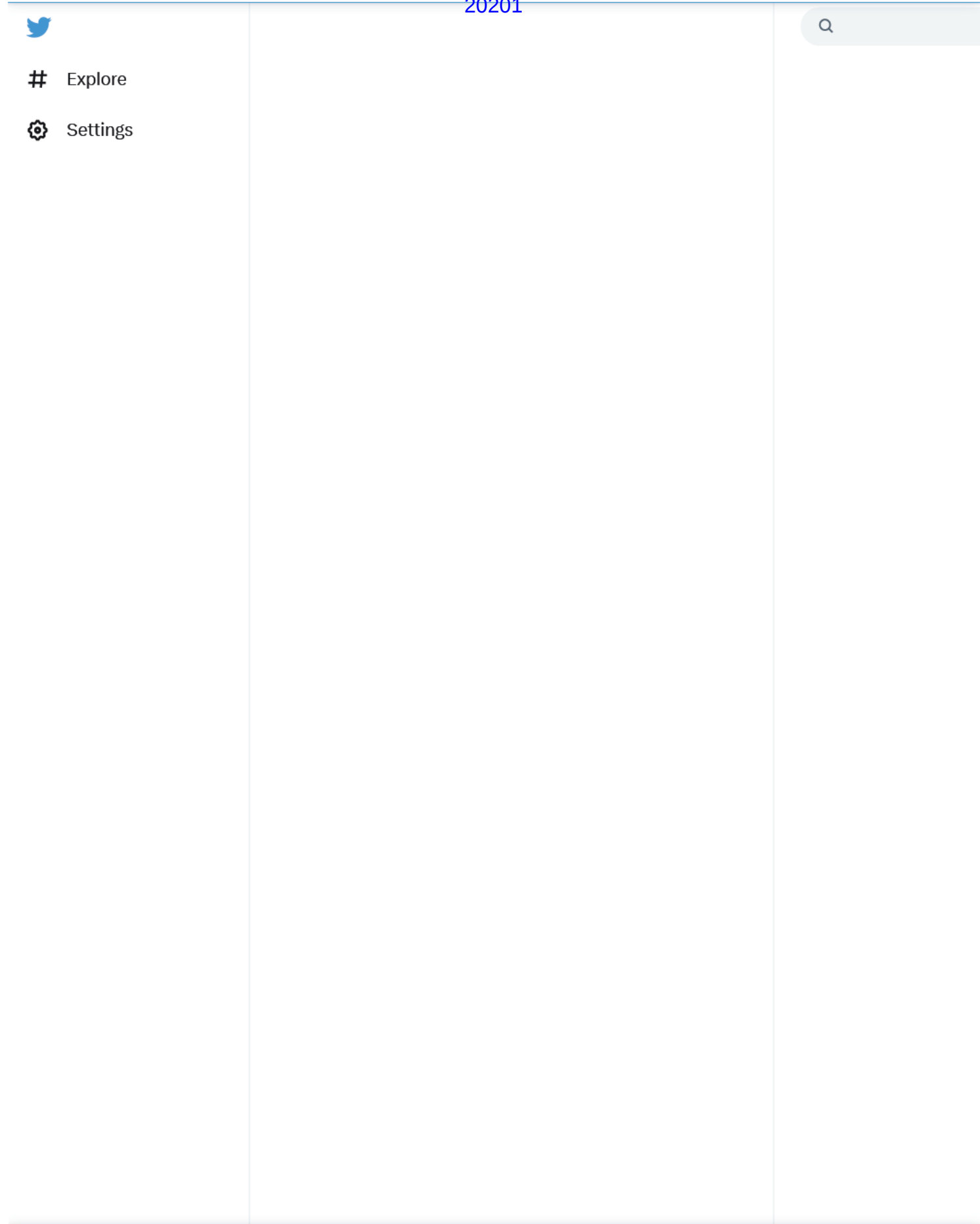
8

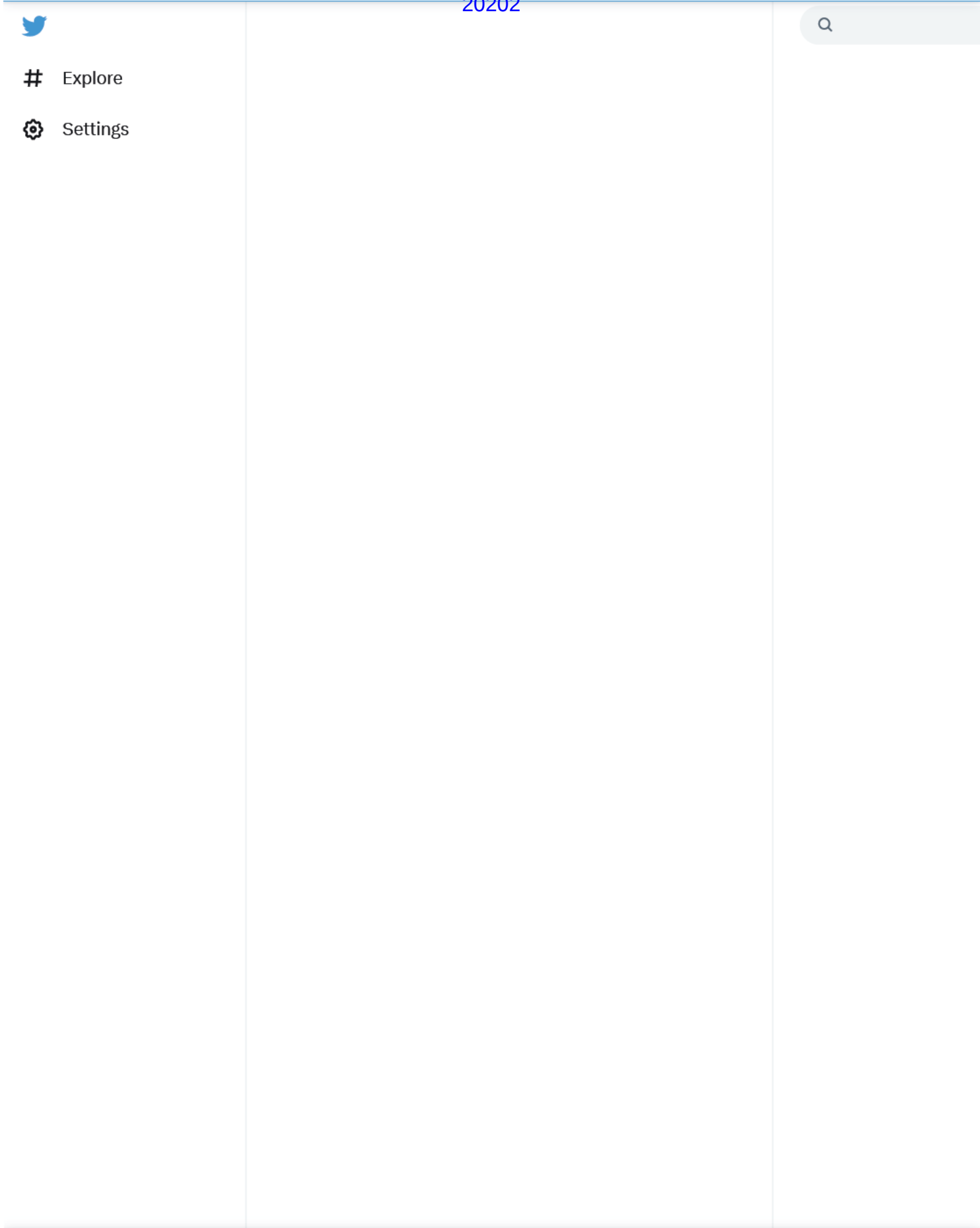
42

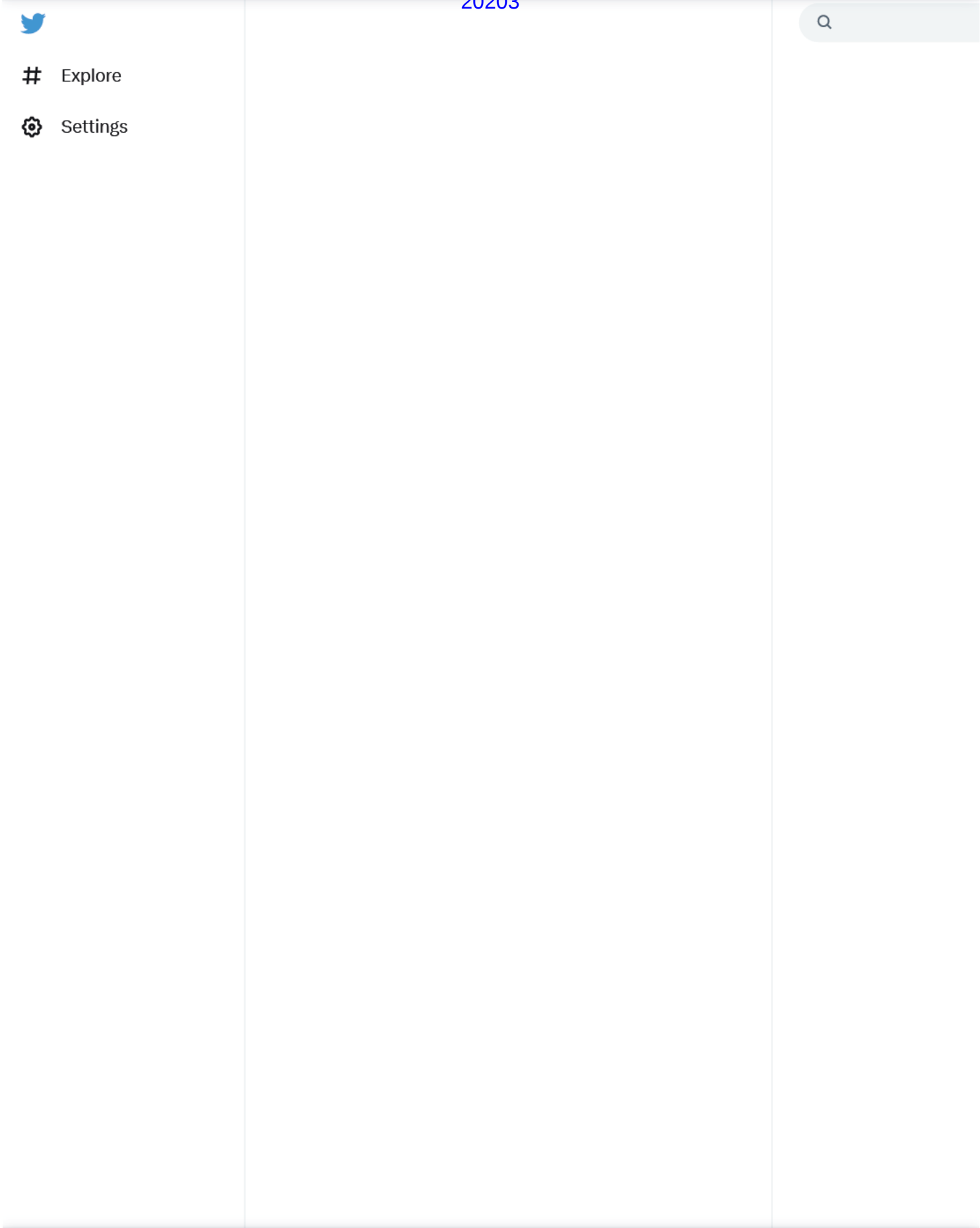
4,525

Show this thread











Explore

⚙ Settings

Don't miss what's happening

People on Twitter are the first to know.

Log in

S

EXHIBIT F



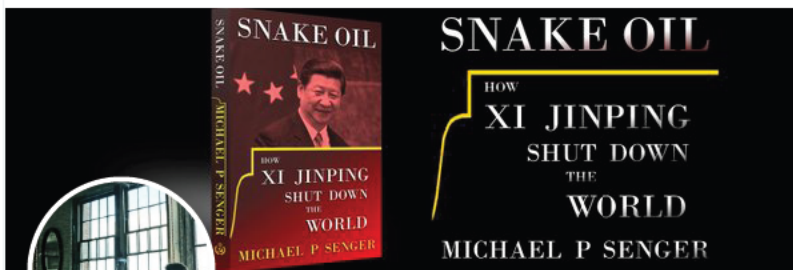
Explore

Settings



Michael P Senger

32.7K Tweets



Follow

Michael P Senger

@MichaelPSenger

Attorney, author of Snake Oil: How Xi Jinping Shut Down the World
amzn.to/33xrGXE

michaelpsenger.substack.com Joined August 2013

23K following 148.9K followers

Tweets

Replies

Media

Likes

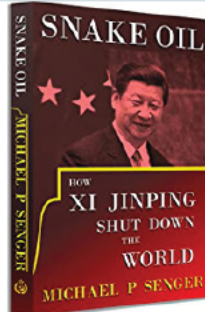
Pinned Tweet



Michael P Senger @MichaelPSenger Oct 31, 2021

Snake Oil: How Xi Jinping Shut Down the World

Through propaganda and fraud, the CCP undermined the snake oil of lockdowns into "science," the greatest crime of the 21st century to date. This is the story of how he did it, and why 1/



★★★★★ 504

amazon.com

Snake Oil: How Xi Jinping Shut Down the World
In March 2020, the democracy ground to a sudden stop. The Reichstag of 1933, historians may never know how AR CoV 2

1,165

11.8K

16.1K



Show this thread



Michael P Senger @MichaelPSenger · 33m

Just how many times has she died of COVID?



collagen machine broke @chronicallybeee · 1h

being immunocompromised/high risk during this pandemic and seeing a lot of society abandon us and decide our deaths are justified for their enjoyment has permanently altered the way I view people and the world. I will never be the same again.



Search Twitter

New to Twitter?

Sign up now to get your own pen



Sign up with G



Sign up with A

Create account

By signing up, you agree to the [Twitter Privacy Policy](#), including [Cookie Policy](#)

You might like



Dr. Simon Goddek

@goddeketal



The Vigilant Fox

@VigilantFox



Chief Nerd

@TheChiefNerd

how many

What's happening

NBA Last night

Suns at Lakers

Trending in United States

TikTok

Trending with ByteDance

Trending in United States

Vertigo

4,012 Tweets

Jungkook · Trending

jungkook

368K Tweets

Sports · Trending

Cancel the WBC

how many

Terms of Service Privacy Policy

Accessibly Ads Info More


© 2022 Twitter Inc

Don't miss what's happening

People on Twitter are the first to know.

Log in


S



Explore

Settings

Michael P Senger Retweeted



@R0b0tSp1der · 1h

Rep ying to @MichaelPSenger and @NanHayworth

've said it from the start:

'm the coming years, they' revise the case and "death" counts down to 5% of what was actual y c aimed.

"Oh, we counted each of 6 tests as separate cases deaths for the same person. Oops."

and so on


1

6

36

2,460

Michael P Senger Retweeted



Steve beck @Stevebe31446528 · 2h

Rep ying to @MichaelPSenger and @DrJBhattacharya

Worse than that they fabricated figures cases deaths, and not sure even the tests were true. t was a massive scam.


1

3

14

1,955

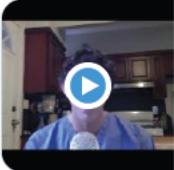
Michael P Senger Retweeted



Susan Prager @SuePrager · 2h

Rep ying to @MichaelPSenger

By the end of March 2020, this NYC ER doc had figured out that the venti ators were more dangerous to hospita ized covid patients than was the virus. He sounded the a arm. He was ignored.




youtube.com
FROM NYC CU: DOES COV D-19 REALLY CAUSE ...
am a physician who has been working at the bedside of COV D+ patients in NYC. be lieve we ...

4

9


30

1,764



Michael P Senger @MichaelPSenger · 2h

Ba aji's 'prophecies' may be the best evidence yet that there was a p an to recreate China's COV D response g oba y, down to the particu ar terms and detai s of how the wor d wou d transform.




michae psenger.substack.com
Ba aji Srinivasan: The Man Who Cou dn't Wait for COV D to Ring n t...
Ba aji's Twitter 'prophecies' may be the best evidence yet that there was a p an to recreate China's COV D response g oba y, down to the...

1

28

31

2,846



Michael P Senger @MichaelPSenger · 2h

The instigators of COV D ockdowns and mandates knew their actions were inde ib y affecting mi ions of ives. The best way we can take "persona responsibi ty" for this catastrophe is to make sure they face a comprehensive inquiry into their decisions.


Don't miss what's happening

Peop e on Twitter are the first to know.

Log in


S


https://twitter.com/MichaelPSenger?ref_src=twsrc%5Egoogle%7Ctwcamp%5Eserp%7Ctwgr%5Eauthor 2/9



Explore

Settings





michaelsengler.substack.com

Corruption and COVID: We Are Not 'All in This Together'

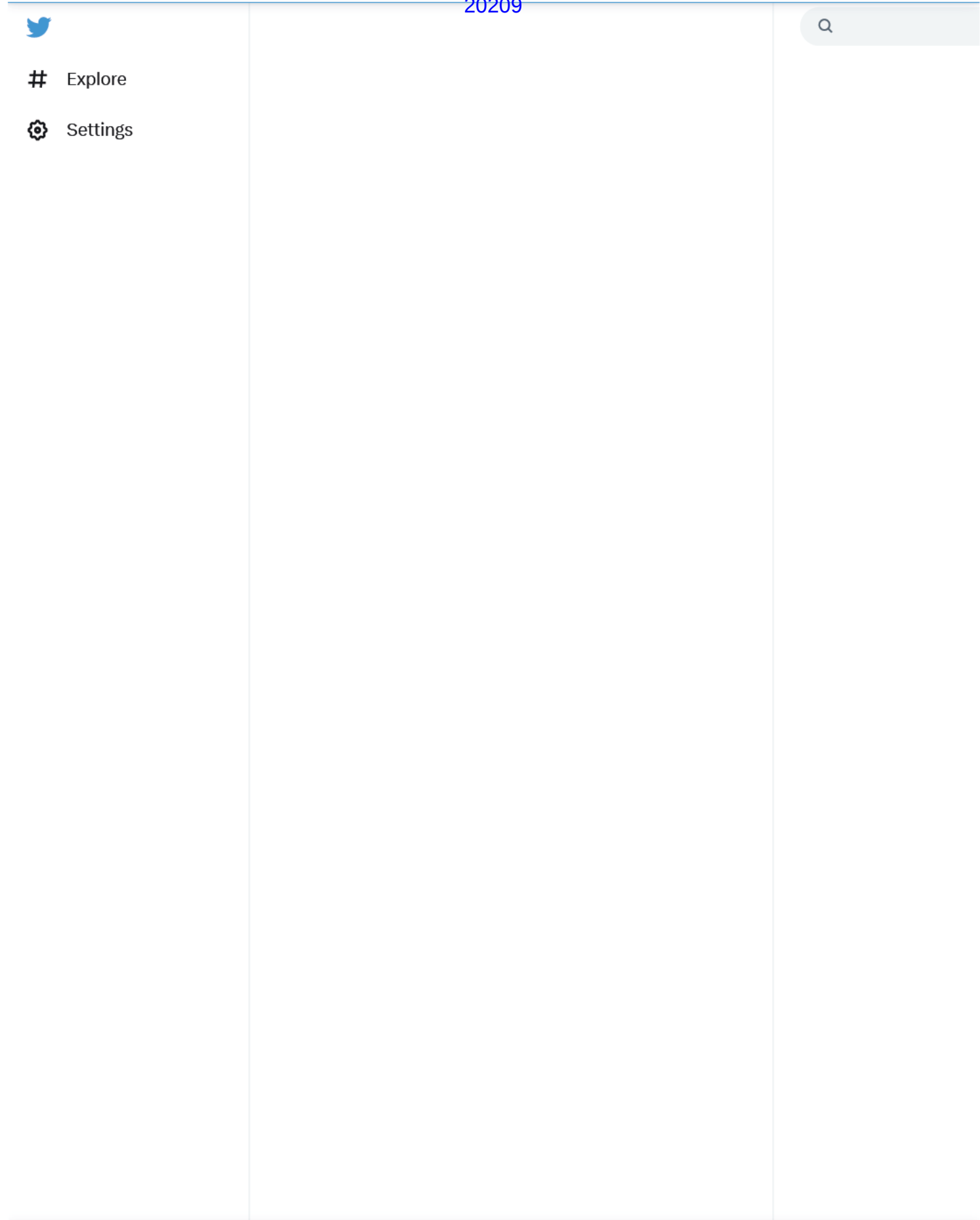
Beware overtures to 'personal responsibility' for the response to COVID, at either the individual or national level. They may be used to...

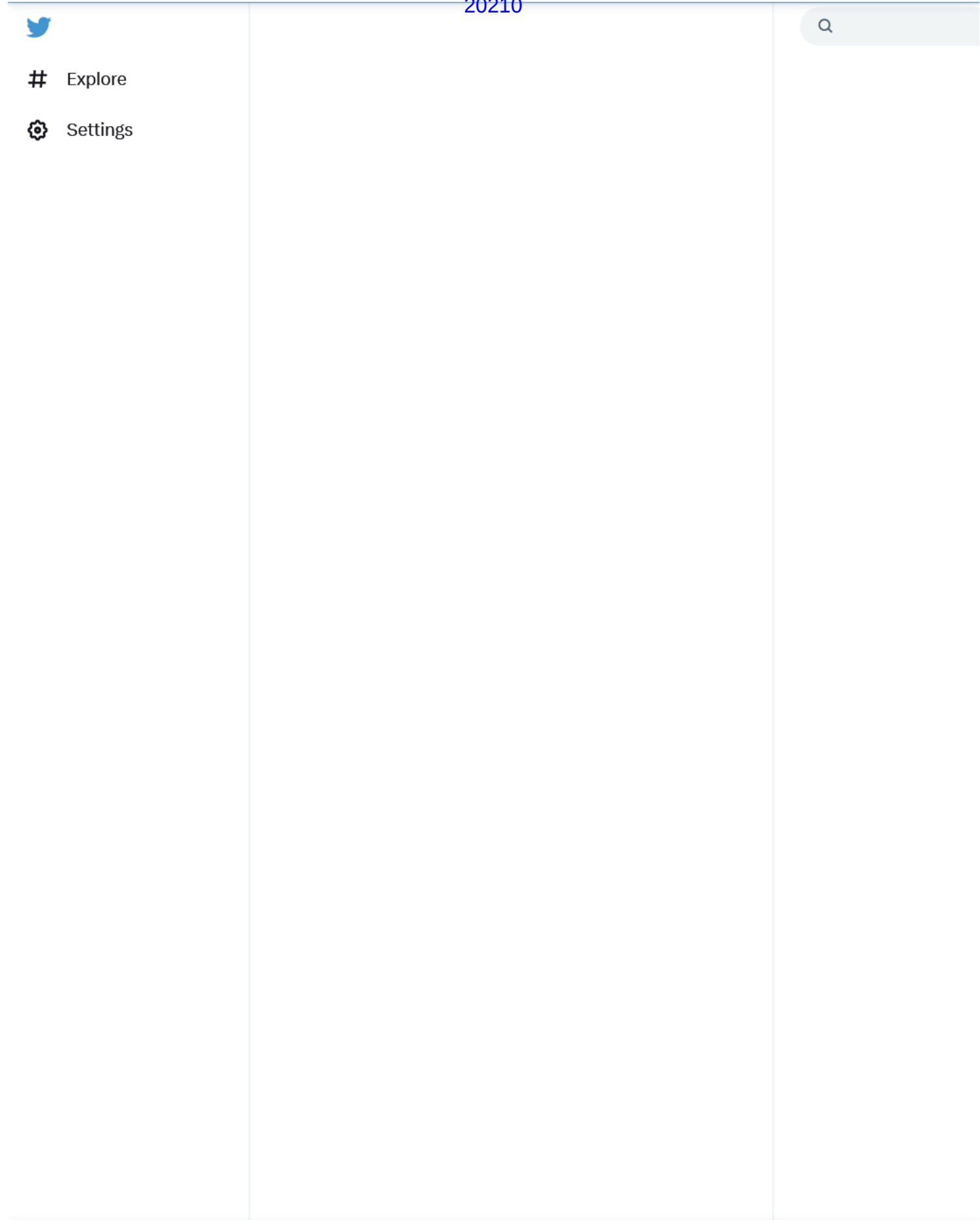
6

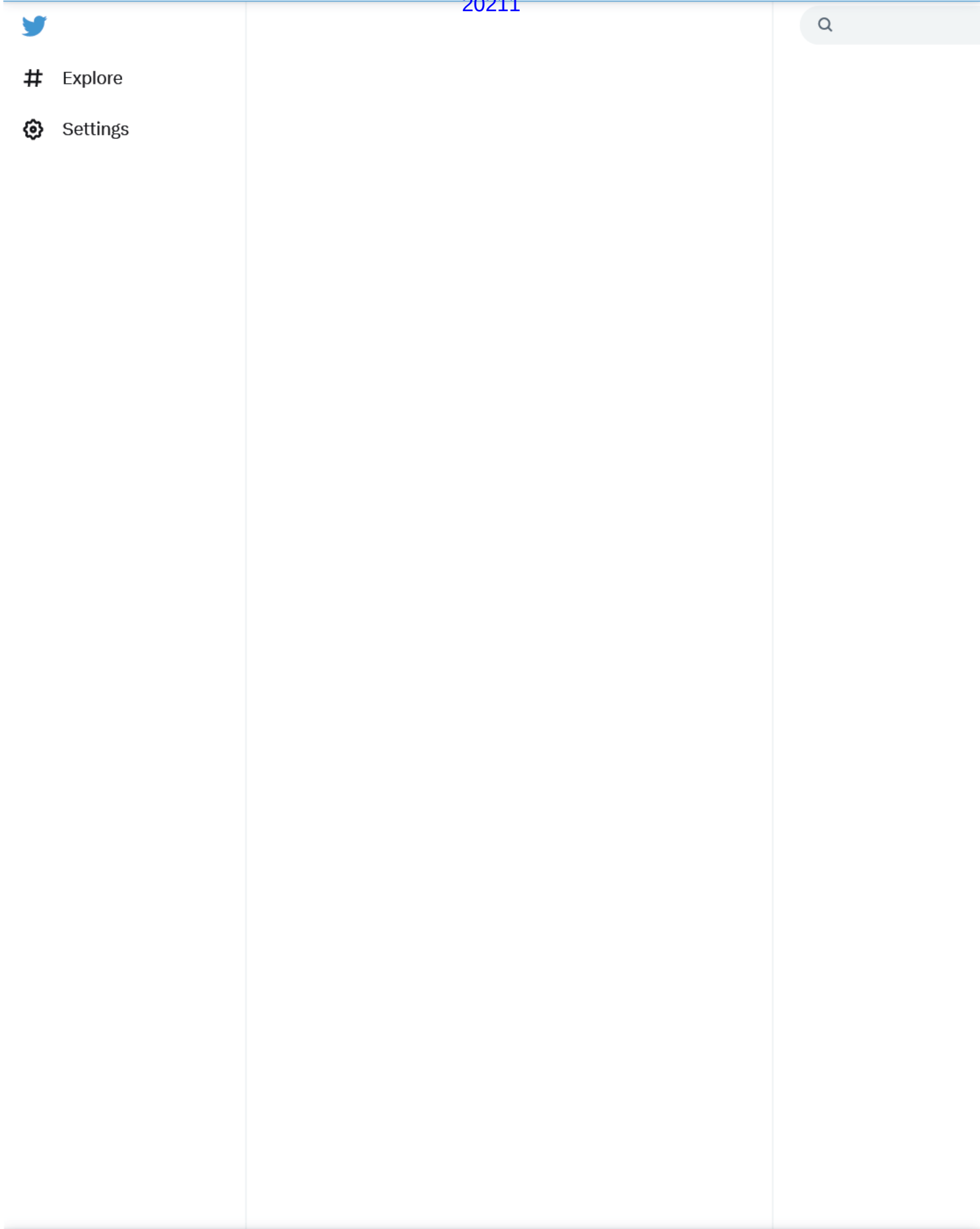
5

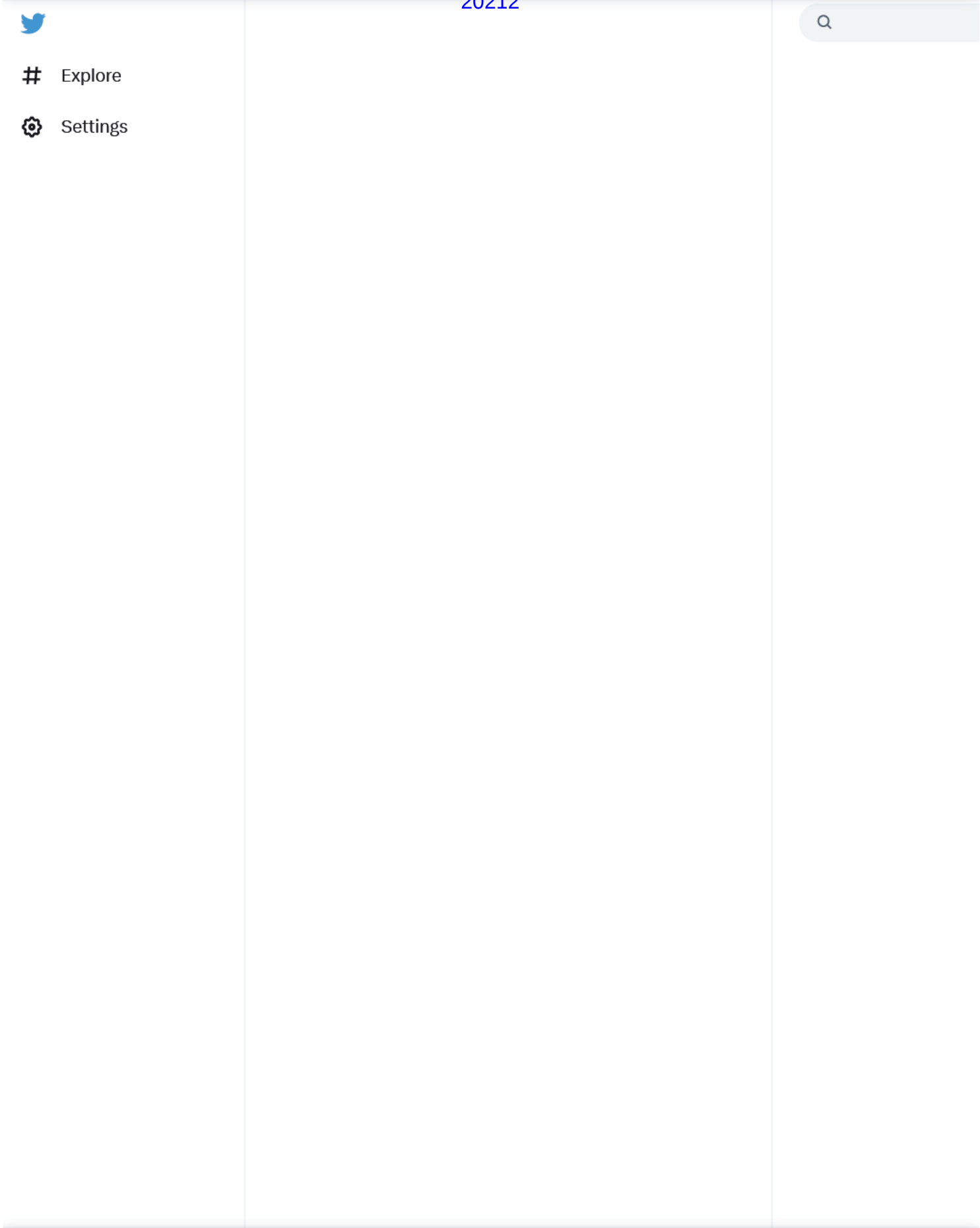
08

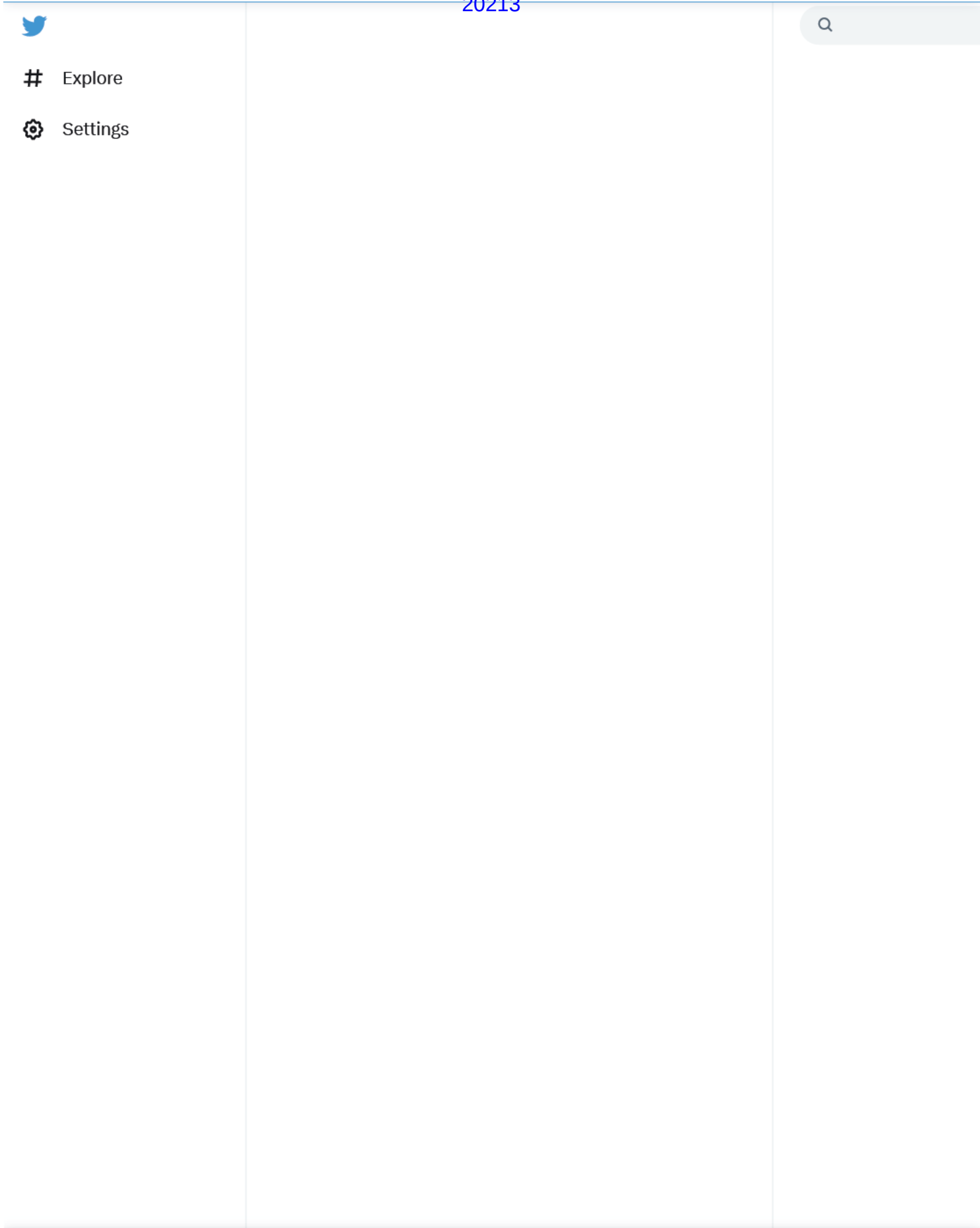
9













Explore

⚙ Settings

Don't miss what's happening

People on Twitter are the first to know.

Log in

S

EXHIBIT G

facebook

Log In

HFL Group

Formerly Baton Rouge Regional



H F L Group(formerly HFL Baton Rouge Regional)

Private group · 505 members

Join group



About

Discussion

About this group

This secret group is a tool to be candid about conversations with Louisiana Legislators. It is also a private place to discuss strategy in orde... See more



Private

Only members can see who's in the group and what they post.



Visible

Anyone can find this group



History

Group created on January 6, 2017. Name last changed on October 7, 2021.




See more

Members · 505

Activity



Log In

-  **No new posts today**
13 in the last month
-  **505 total members**
No new members in the last week
-  **Created 6 years ago**

Group rules from the admins

- 1 **Let's stay connected!!!** ^

Please sign up for email and voter voice, and join our telegram channel. There will be a post in the announcements with links.
- 2 **Code words.** ^

Some words are off limits. You know what to do.
- 3 **No links in original posts.** ^

To help keep our group up and functioning, please do not post any links in posts. Once your post is approved, you can put links in the comments.
- 4 **Not all posts will be approved.** ^

Not all posts will be approved. Please don't be offended!!
Two of our groups have been taken down - we are going to be very selective.
- 5 **Be kind and courteous** ^

We're all in this together to create a welcoming environment. Let's treat everyone with respect. Healthy debates are natural, but kindness is required.
- 6 **No hate speech or bullying** ^

Make sure everyone feels safe. Bullying of any kind isn't allowed, and degrading comments about things like race, religion, culture, sexual orientation, gender or identity will not be tolerated.
- 7 **No promotions or spam** ^



Log In

8 **Respect everyone's privacy**

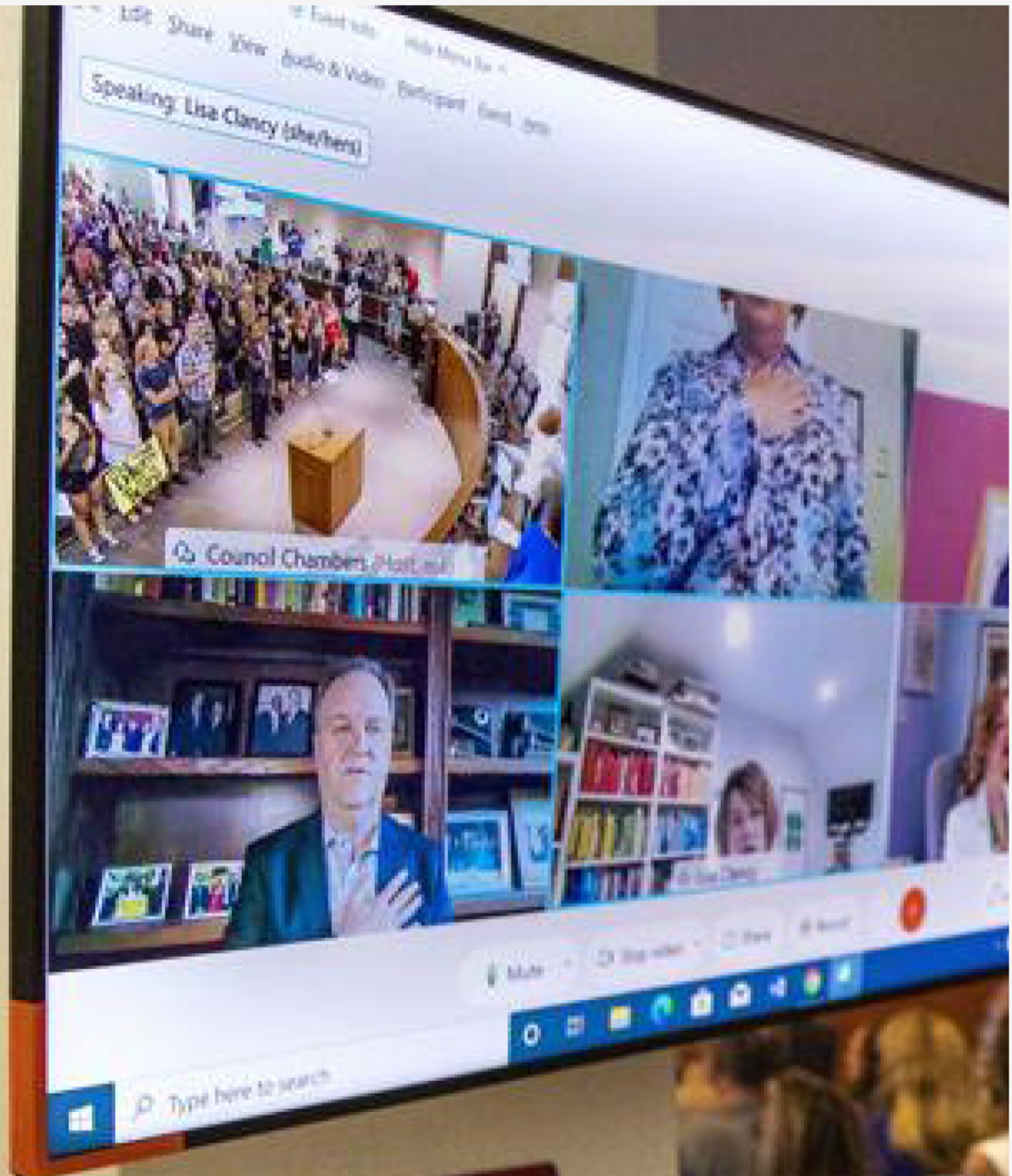


Being part of this group requires mutual trust. Authentic, expressive discussions make groups great, but may also be sensitive and private. What's shared in the group should stay in the group.

EXHIBIT H

Misinformation at public forums vexes local boards, big tech

By DAVID KLEPPER and HEATHER HOLLINGSWORTH August 16, 2021





KANSAS CITY, Mo. (AP) — There are plenty of places to turn for accurate information about COVID-19. Your physician. Local health departments. The U.S. Centers for Disease Control.

But not, perhaps, your local government’s public comment session.

During a meeting of the St. Louis County Council earlier this month, opponents of a possible mask mandate made so many misleading comments about masks, vaccines and COVID-19 that YouTube removed the video for violating its policies against false claims about the virus.

“I hope no one is making any medical decisions based on what they hear at our public forums,” said County Councilwoman Lisa Clancy, who supports mask wearing and said she believes most of her constituents do too. The video was restored, but Clancy’s worries about the impact of that misinformation remain.

Coronavirus pandemic



Ignoring experts, China's sudden zero-COVID exit cost lives

Ignoring experts, China's sudden zero-COVID exit cost lives

North Carolina House advances ban on COVID vaccine mandates

Anthony Fauci documentary on PBS covers a career of crises

Biden signs bill on COVID origins declassification

Videos of local government meetings have emerged as the latest vector of COVID-19 misinformation, broadcasting misleading claims about masks and vaccines to millions and creating new challenges for internet platforms trying to balance the potential harm against the need for government openness.

ADVERTISEMENT

The latest video to go viral features a local physician who made [several misleading claims about COVID-19](#) while addressing the Mount Vernon Community School Corporation in Fortville, Indiana, on Aug. 6. In his 6-minute remarks, Dr. Dan Stock tells the board that masks don't work, vaccines don't prevent infection, and state and federal health officials don't follow the science.

The video has amassed tens of millions of online views, and prompted the Indiana State Department of Health to push back. Stock did not return multiple messages seeking comment.

“Here comes a doctor in suspenders who goes in front of the school board and basically says what some people are thinking: the masks are B.S., vaccines don't work and the CDC is lying — it can be very compelling to laypeople,” said Dr. Zubin Damania, a California physician who received so many messages about the Indiana clip that he created his own video debunking Stock's claims.

Damania hosts a popular online medical show under the name ZDogMD. His video debunking Stock's comments has been viewed more than 400,000 times so far. He said that while there are legitimate questions about the effectiveness of mask requirements for children, Stock's broad criticism

of masks and vaccines went too far.

YouTube removed several similar videos of local government meetings in North Carolina, Missouri, Kansas and Washington state. In Bellingham, Washington, officials responded by temporarily suspending public comment sessions.

ADVERTISEMENT

The false claims in those videos were made during the portion of the meeting devoted to public comment. Local officials have no control over what is said at these forums, and say that's part of the point.

In Kansas, YouTube pulled video of the May school board meeting in the 27,000-student Shawnee Mission district in which parents and a state lawmaker called for the district to remove its mask mandate, citing "medical misinformation."

The district, where a mask mandate remains in effect, responded by ending livestreaming of the public comment period. District spokesman David Smith acknowledged that it has been challenging to balance making the board meetings accessible and not spreading fallacies.

"It was hard for me to hear things in the board meeting that weren't true and to know that those were going out without contradiction," Smith said. "I am all about free speech, but when that free speech endangers people's lives, it is hard to sit through that."

After hearing from local officials, YouTube reversed its decision and put the videos back up. Earlier this month the company, which is owned by Google, announced a change to its COVID misinformation policy to allow exceptions for local government meetings — though YouTube may still remove content

that uses remarks from public forums in an attempt to mislead.

“While we have clear policies to remove harmful COVID-19 misinformation, we also recognize the importance of organizations like school districts and city councils using YouTube to share recordings of open public forums, even when comments at those forums may violate our policies,” company spokeswoman Elena Hernandez said.

The deluge of false claims about the virus has challenged other platforms too. Twitter and Facebook each have their own policies on COVID-19 misinformation, and say that like YouTube they attach labels to misleading content and remove the worst of it.

Public comment sessions preceding local government meetings have long been known for sometimes colorful remarks from local residents. But before the internet, if someone were to drone on about fluoride in the drinking water, for instance, their comments weren’t likely to become national news.

Now, thanks to the internet and social media, the misleading musings of a local doctor speaking before a school board can compete for attention with the recommendations of the CDC.

It was only a matter of time before misleading comments at these local public forums went viral, according to Jennifer Grygiel, a communications professor at Syracuse University who studies social media platforms.

Grygiel suggested a few possible ways to minimize the impact of misinformation without muzzling local governments. Grygiel said clear labels on government broadcasts would help viewers understand what they’re watching. Keeping the video on the government’s website, instead of making it shareable on YouTube, could allow local residents to watch without enabling the spread of videos more widely.

“Anytime there is a public arena – a city council hearing, a school board meeting, a public park – the public has the opportunity to potentially spread misinformation,” Grygiel said. “What’s changed is it used to stay local.”

Klepper reported from Providence, Rhode Island.

ADVERTISEMENT

You May Like

Promoted

Amazon Left Scrambling As Prime Users Find Out About Secret Deals

Promoted: Online Shopping Tools

2 Insane Cards Charging 0% Interest Until Nearly 2025

Promoted: CompareCredit.com

[Learn More](#)

Minneapolis: Luxury Walk-In Tubs Are Almost Being Given Away: See Prices

Promoted: Baths On Clearance | search ads

Limited time offer - Gucci glasses are now on sale

Promoted: GlassesUSA.com

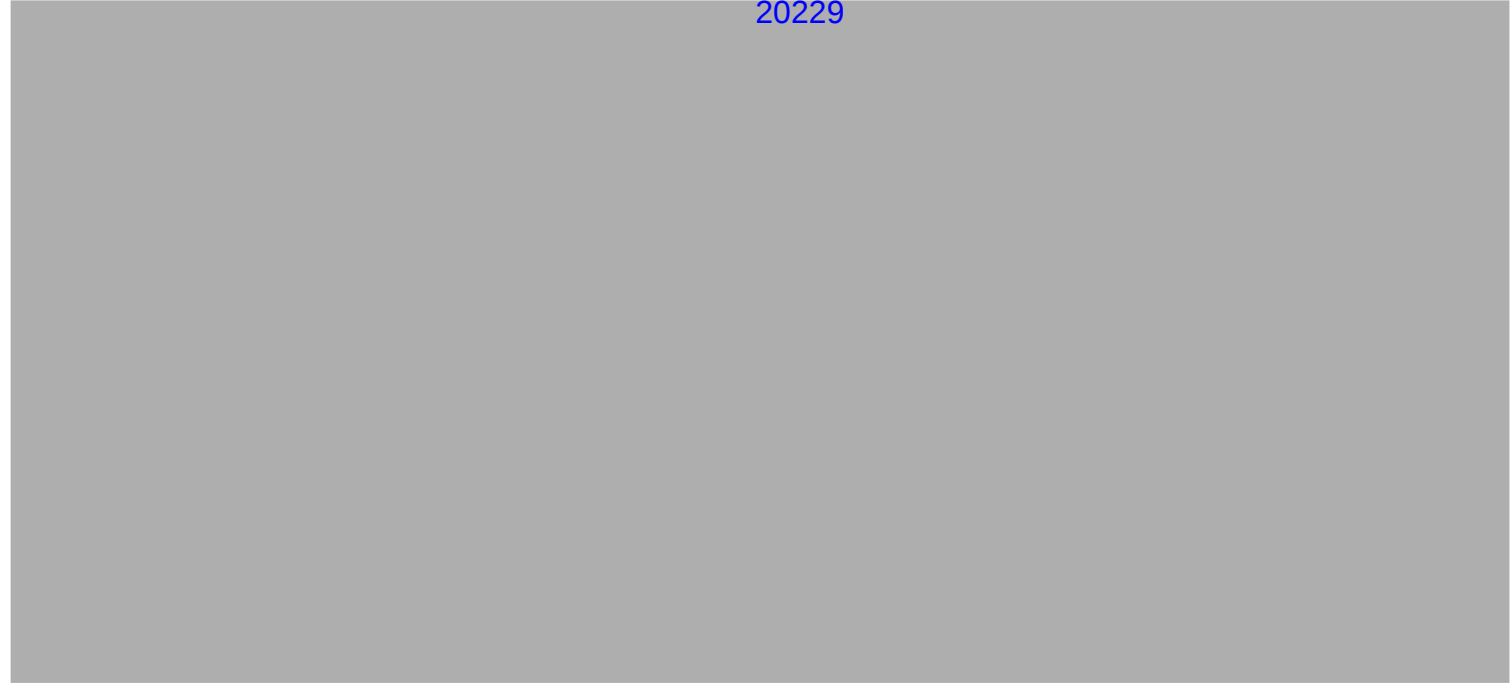
Shop Now

by Taboola

ADVERTISEMENT

You May Like

by Taboola



Ad Content

Amazon Hates When Prime Members Do This, But They Can't Stop You

Online Shopping Tools

The Killer New Audi E-Tron Has Arrived: See Specs,...

Audi E-Tron | Search Ads

Learn More

Killer New EVs That Many Don't Realize Are Affordable

New Electric Cars | Search Ads

Empty Alaska Cruise Cabins Cost Almost Nothing

Alaska Cruise Deals | sponsored searches

Introducing The Wives Of The Richest Men in the World

Wanderoam

“These ADHD Drops Make You Feel Great And Think...

Health Headlines

Learn More

Ad Content

The World’s Most Advanced Smartwatch Is Here

Promoted: Rival

Learn More

The Luxurious New Honda Has Arrived

Promoted: Best Honda Deals | Search Ads

Learn More

BMW's Killer 2023 X5 Lineup Is Finally Here

Promoted: The New BMW X5

Photo of Plymouth Rock misrepresented to

CLAIM: A photo of

yesterday

Ad Content

The Killer New BMW X7 Has Arrived: See Specs, Prices,...

Auto Savings Center | Search Ads

Learn More

Yellowstone Discontinued - Effective Immediately

investing.com

Major Airlines Don't Want You To Know How Cheap Flying Private Actually Is

Jets For Less

Learn More

Minneapolis: Unsold Never-Driven Cars Now Almost Being Given Away: See...

SUV Deals | Search Ads

These Vegetables Will Kill Your Belly And Arm Fat...

Fitness

Gwen Stefani, 53, Takes Off Makeup, Leaves Us With N...

Finance Wealth Post

Ad Content

Play Today For Free

Promoted: Chumba Casino

Are you our next millionaire?

Promoted: Chumba Casino

New BMWs Basically on Clearance Sale

Promoted: Hot Deals - Top Searches

[Learn More](#)

Trump loses last bid to keep key evidence out of rape trial

NEW YORK (AP) — Former President Donald Trump's effort to keep key evidence out of his ...

March 20, 2023

AP NEWS

[Top Stories](#)

[Video](#)

[Contact Us](#)

[Accessibility Statement](#)

[Cookie Settings](#)

DOWNLOAD AP NEWS

Connect with the definitive source for global and local news

MORE FROM AP

[ap.org](#)

[AP Insights](#)

[AP Definitive Source Blog](#)

[AP Images Spotlight](#)

[AP Explore](#)

[AP Books](#)

[AP Stylebook](#)

FOLLOW AP

THE ASSOCIATED PRESS

[About](#)

[Contact](#)

[Customer Support](#)

[Careers](#)

[Terms & Conditions](#)

[Privacy](#)

All contents © copyright 2023 The Associated Press. All rights reserved.

EXHIBIT I

Explore

Settings

←

Mark Changizi

113.6K Tweets

Follow

Mark Changizi

@MarkChangizi

Cognitive Scientist, changizi.com — Free Expression Institute, FreeX.group — Vein Finder & Co orb ind G asses, VinoOptics.com

Science & Technology

Miami, FL

markchangizi.substack.com

Joined June 2009

1,895 Following

53.9K Followers

Tweets

Replies

Media

Likes

Pinned Tweet

Mark Changizi

@MarkChangizi · Feb 14

pin thread

After 20 months of being labeled sensitive content by Twitter for arguing against the Covid interventions, they stopped censoring me yesterday.

So I'm starting a new pinned thread, beginning with my pinned tweet since Covid began.

Mark Changizi

@MarkChangizi · Mar 17, 2020

The moral of coronavirus 19 was that social contagion via social networks is more dangerous than biological contagion

[how this thread](#)

27

132

459

70.3K

Show this thread

Mark Changizi Retweeted

Mazda Sabouri

@msabouri · 1h

choose covid social science

Search Twitter

New to Twitter?

Sign up now to get your own pen

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the [Twitter Privacy Policy](#), including [Cookie Policy](#)

You might like

Gain of Fauci

@schoesIsac

Dr. Tess Lawrie

@awed

Dr. Simon Goddek

@goddetta

[how more](#)

What's happening

NHL Last night

Panthers at Bruins

Music · Trending

eunwoo

167K Tweets

Trending in United States

Emergency Broadcast Sys

1,343 Tweets

Music · Trending

#MoonBinWeLoveYou

26.2K Tweets

Entertainment · Trending

Damson Idris

7,823 Tweets

Don't miss what's happening


People on Twitter are the first to know.

Log in

S


https://twitter.com/MarkChangizi


1/9



Explore

Settings


**Mark Changizi** @Ma Chang z 33m


**Damian** @raggedlines · 4h

t s a great shame that most of the retrospective criticism for vaccine mandates & coercion is fue ed by how use ess and potentia y harmfu the vaccines turned out to be and not how comp ete y immora and unjust those mandates & coercion were regard ess of the vaccines efficacy

2

766

**Mark Changizi** @MarkChangizi · 43m

**Dr Ben Irvine** @BenIrvineAuthor · 53m


How on this earth can it be possib e to supp y a mountain of evidence of what ACTUALLY caused the c osures in Britain, yet the vast majority of ockdown sceptics prefer a weird paranoid hypothesis for which zero evidence has EVER been given? My brain exp odes at the paradox. [twitter.com/BenIrvineAutho...](https://twitter.com/BenIrvineAuthor)

1

6

921

Mark Changizi Retweeted


**Ryan Lawrence** @RyanLawrence2 · 1h

Re y ng to [@vtoVanc n](#) and [@Ma Chang z](#)

Rem nds me of th s s eech thomas mass e osted yeste day He s usua y one of ve y few n gove nment t y ng to sto those good ntent ons from ecom ng aw

**Thomas Massie** @RepThomasMassie · 17h

We do not need E-Verify, or other federa databases ike N CS, Rea D, No-f y ists, and centra bank digita currencies, in order for aw-abiding Americans to exercise their fundamenta human rights.




5

0

80

Mark Changizi Retweeted

**Vito Vancini** @vitovancini · 20h

Rep ying to [@MarkChangizi](#)

The phenomenon, ike a authoritarianism, began with peop e who though they were doing good with p ausib e sounding po icies and morphed into something ug y with a life of its own. Once it had that momentum, it was impossib e to stop.

1

4

7

674

Mark Changizi Retweeted

**Mark Changizi** @MarkChangizi · 21h


Don't miss what's happening

Peop e on Twitter are the first to know.

Log in



S

https://twitter.com/MarkChangizi 2/9



Explore

Settings

**Shelby**  @wildtrailflow · 21h



Rep ying to @MarkChangizi



For a ot of peop e the idea that no one is in contro is too terrifying to contemp ate.

2

6

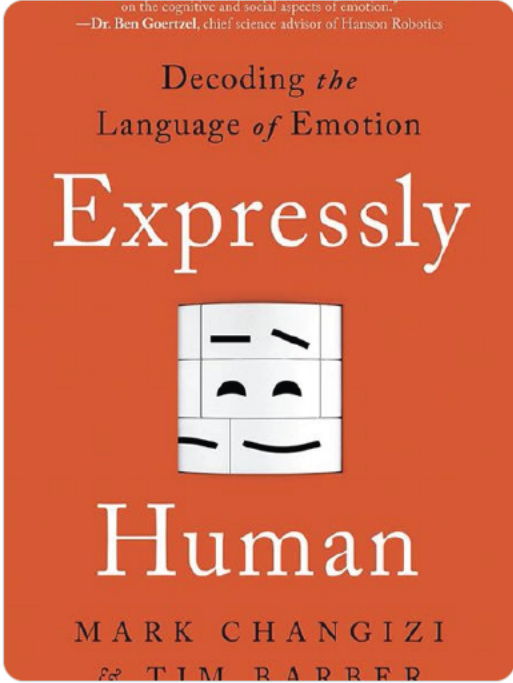
2 520

**Mark Changizi**  @MarkChangizi · 21h

 The government censored @DrTimBarber and my book, ten years in the making. 

Get yourse ves a copy of my sixth and most important book, on the foundations of free expression and human socia networks.

f you have a ready read it, give it a review at Amazon.... [Show more](#)



1

21

46

6,472

EXHIBIT J

4/24/23 9:01 AM

Robert W Malone, MD (@RWMaloneMD) / Page 186 of 672

20239



Twitter

Explore

Settings

Robert W Malone, MD

12.6K Tweets



Follow

Robert W Malone, MD

@RWMaloneMD

inventor/skeptic mRNA vaccines. Scientist. Author. Speaker. Bioethicist.
rwma.onemd.substack.com
ma.oneinstitute.org
rwma.onemd.com
imdb.com/name/nm5374331

Madison, VA rwma.onemd.substack.com Joined May 2009

960 following 1M followers

Tweets

Replies

Media

Likes

Pinned Tweet

Robert W Malone, MD

@RWMaloneMD


23h

...

unday t The Mode n Wo d

m e s e t t e ?

stac at RWMaloneMD



wma.onemd.substack.com

unday t The Mode n Wo d

m e s e t t e ?

7

33

129

35.5K


Robert W Malone, MD

@RWMaloneMD

42m

...

My newest essay is now published. Due to the censorship on Twitter, I am no longer sure how many people can actually get to the link. Click on the link, not the image. So, here goes: tinyurl.com/5az6cfv8



Search Twitter

New to Twitter?

Sign up now to get your own profile

Sign up with Google

Sign up with Apple

Create account

By signing up, you agree to the Terms of Service and Privacy Policy, including Cookies

PsyWars

The 21st Century Battlefield

The Modern World in a Single

I'm Eating the Bugs

DO CHANGE THE WEATHER

You might like

Robert F. Kennedy

@RobertKennedy

O'Keefe Media Group

@OKeefeMedia

The Babylon Bee

@TheBabylonBee

how many

What's happening

NBA Last night

Nuggets at Timberwolves

Politics - Trending

Trump

552K Tweets

Politics - Trending

Om Shanti

7,615 Tweets

Korean music - Trending

seungkwan

105K Tweets

Entertainment - Trending

Darth Maul


2,663 Tweets

Don't miss what's happening

People on Twitter are the first to know.

Log in

S



Explore


Settings

2

86


20

8K



Robert W Malone, MD @RWMaloneMD · 1h

Clean vs. Dirty: A Way to Understand Everything • Brownstone Institute. Great insight!



brownstone.org

Clean vs. Dirty: A Way to Understand Everything • Brownstone Institute... The clean vs. dirty distinction was once an indicator of class, perhaps a desiderata of germaphobic pathology, even a harmless eccentricity.


10

75

213


28.9K

Robert W Malone, MD Retweeted



Jan Jekielek @JanJekielek · 2h

This is unconscionable, deeply unethical, and even in a cold, dark, inhumane world, would make no sense given what we know of the science of COVID and the genetic vaccines



The Epoch Times @EpochTimes · 12h

On diagnosis and potentially facing death, a 41-year-old homeschooling mother of 7 young children has been rejected as a candidate for a life-saving kidney transplant.


The reason? She refused to receive a #COVID19 vaccine on religious and medical grounds. theepochtimes.com/mother-of-7-de...

29

298

695

51K



Robert W Malone, MD @RWMaloneMD · 2h

Brazil's greatest living scientist is unanimously acquitted by medical councils. The translator program made a mess of the headline but didn't catch the errors.


3

66

448

30.5K

Show this thread



Robert W Malone, MD @RWMaloneMD · 10h

Fantastic News!
Brazil's greatest living scientist is universally acquired by medical councils
Dr Flavio Cadegiani... found the world's most effective treatment for hospitalized COVID-19 patients...
tinyurl.com/3zc99pwt

87

1,071

3,593

193.9K

Don't miss what's happening
People on Twitter are the first to know.

Log in

S

https://twitter.com/RWMaloneMD 2/9

Explore

Settings

n 2019, the com any went a n on G Othe home stores th ved du ng cov d

Cong ats to @ ed ath eyond fo ta ng the ca on foot nt to ze o

A Message to Our Stakeholders:

On behalf of our 60,000 Associates serving customers in more than 1,500 stores in the United States, Puerto Rico and Canada, we are pleased to present Bed Bath & Beyond's 2019 Corporate Responsibility Report. Since we first opened our doors in 1971, Bed Bath & Beyond's top priority has been our commitment to customer service and being a responsible corporate citizen, which remains true today.

The past year, our teams have been focused on driving the Company's transformation efforts and

finding new ways to delight our customers, enhance our competitive position, improve our financial performance, and drive shareholder value. While progress has been made, there is still more work to be done. During 2019, we also significantly transformed Bed Bath & Beyond's Board governance structure, reduced the appointment of our new independent directors with senior female directors, a mix diversity of perspectives, backgrounds, ages, gender race and ethnicity. As a result of these changes, our Board better reflects the diversity of the Company's loyal customers and dedicated Associates.

As we evolve our business, we will continue to improve our approach to corporate social responsibility and the way in which we communicate with stakeholders. This year's Corporate Responsibility Report is presented in a more streamlined, user-friendly format and highlights the areas in which we have been making meaningful strides, and we look forward to improving our performance and disclosures on environmental, social, and governance issues in the future.

The Wall Street Journal @WSJ · Apr 23

Breaking: Bed Bath & Beyond fi ed for bankruptcy protection from creditors after years of osses and a fai ed turnaround p an on.wsj.com/3KWYsDz

82

27

9

7K

DEFENDANTS' EXHIBIT 140:

From: Flaherty, Rob EOP/WHO [/O=EXCHANGE ORGANIZATION/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=E651A028571D49DFB77F078E7A223D1D-FL]
Sent: 4/12/2021 9:55:41 PM
To: Todd O'Boyle [toboyle@twitter.com]
CC: Lauren Culbertson [lculbertson@twitter.com]; Reggie McCrimmon [reggie@twitter.com]; Qureshi, Hoor EOP/WHO [Hoor.Qureshi@who.eop.gov]
Subject: Checking in on Misinfo and Vaccine Hesitancy

All --

Hope you're well. As we shift from a position where we're moving from a supply problem, into a demand problem, we thought it might be good to check in on your efforts to combat vaccine hesitancy and misinformation.


We're most interested in the following:

- Trends that you're seeing generally around vaccine misinformation
- The material effects you're seeing from your recent policy changes
- What interventions you might currently be trying in addition to previous policy changes
- Ways the White House (and our COVID experts) can partner in your product work

We're still working on the cross-industry stuff, and hopefully have more there soon. If you could send some times over, that'd be great, and Hoor can help wrangle folks on our end.

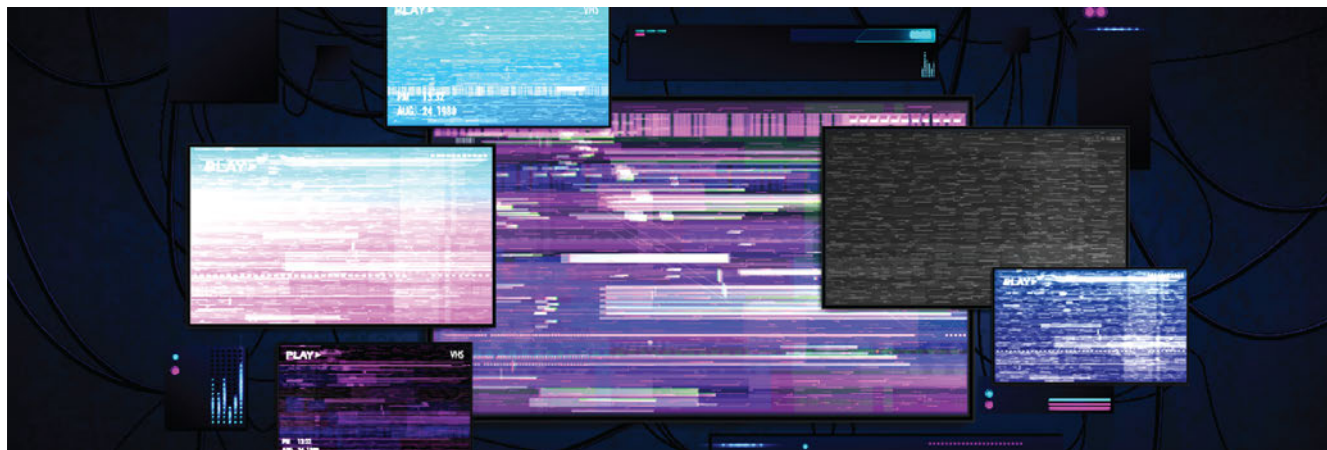
-Rob

DEFENDANTS' EXHIBIT 141:

 An official website of the United States government
Here's how you know

Menu

SHARE:



Foreign Influence Operations and Disinformation

Election Security

Overview

CISA reduces risk to U.S. critical infrastructure by building resilience to foreign influence operations and disinformation. Through these efforts, CISA helps the American people understand the scope and scale of these activities targeting election infrastructure and enables them to take action to mitigate associated risks.

CISA's Role

CISA helps the American people understand the risks from foreign influence operations and disinformation and how citizens can play a role in reducing the impact of it on their organizations and communities. This work is done in close partnership with the interagency, private sector, academia, and international stakeholders.

Guiding Principles

The guiding principles for addressing risk from foreign influence operations and disinformation include the protection of privacy, free speech, and civil liberties. CISA works with its Privacy Office and Office for Civil Rights and Civil Liberties to ensure these principles are reflected in all of its activities.

We are also committed to collaboration with partners and stakeholders. In addition to civil society groups, researchers, and state and local government officials, we work in close collaboration with the FBI's Foreign Influence Task Force, the U.S. Department of State, the U.S. Department of Defense, and other agencies across the federal government. Federal Agencies respective roles in recognizing, understanding, and helping manage the threat and dangers of foreign influence operations and disinformation activities on the American people are mutually supportive, and it is essential that we remain coordinated and cohesive when we engage stakeholders.

Terms to Know

Some tactics of foreign influence include leveraging misinformation, disinformation, and malinformation. Definitions for each are below.

- **Misinformation** is false, but not created or shared with the intention of causing harm.
- **Disinformation** is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.
- **Malinformation** is based on fact, but used out of context to mislead, harm, or manipulate. An example of malinformation is editing a video to remove important context to harm or mislead.

Foreign actors use misinformation, disinformation, and malinformation campaigns to cause chaos, confusion, and division. These malign actors are seeking to interfere with and undermine our democratic institutions and national cohesiveness.

Featured Content

[Tactics of Disinformation](/sites/default/files/publications/tactics-of-disinformation_508.pdf) </sites/default/files/publications/tactics-of-disinformation_508.pdf>

Provides an overview of the 8 most common foreign influence and disinformation tactics used to manipulate the information environment.

[Resilience Series Graphic Novels](/topics/election-security/foreign-influence-operations-and-disinformation/resilience-series-graphic-novels) </topics/election-security/foreign-influence-operations-and-disinformation/resilience-series-graphic-novels>

The Resilience Series Graphic Novels highlights the importance of evaluating information sources to help individuals understand the risks from foreign influence

operations on our society and democracy.

Election Security Rumor vs. Reality </rumor-vs-reality>

Rumor vs. Reality provides accurate and reliable information on common disinformation narratives that relate to the security of election infrastructure.

Related Resources

PUBLICATION

CISA Insights: Preparing for and Mitigating Foreign Influence Operations Targeting Critical Infrastructure </resources-tools/resources/cisa-insights-preparing-and-mitigating-foreign-influence-operations>

PUBLICATION

Rumor Control Start-Up Guide </resources-tools/resources/rumor-control-start-guide>

Foreign Influence Operations and Disinformation

Contact Us

For additional information on our work, please email
electionsecurity@cisa.dhs.gov

CONTACT US

[Return to top](#)

Topics </topics>

Spotlight </spotlight>

Resources & Tools </resources-tools>

News & Events </news-events>

Careers </careers>

About </about>

CISA Central

888-282-0870

Central@cisa.dhs.gov

CISA.gov

An official website of the U.S. Department of Homeland Security

[About CISA </about>](#)

[Accessibility <https://www.dhs.gov/accessibility>](https://www.dhs.gov/accessibility)

[Budget and Performance](#)

[DHS.gov <https://www.dhs.gov>](https://www.dhs.gov)

<https://www.dhs.gov/performance-financial-reports>

[FOIA Requests <https://www.dhs.gov/foia>](https://www.dhs.gov/foia)

[No FEAR Act </cisa-no-fear-act-reporting>](#)

[Office of Inspector General](#)

[Privacy Policy </privacy-policy>](#)

<https://www.oig.dhs.gov/>

[Subscribe](#)

[The White House <https://www.whitehouse.gov/>](https://www.whitehouse.gov/)

[USA.gov <https://www.usa.gov/>](https://www.usa.gov/)

[Website Feedback </forms/feedback>](#)

DEFENDANTS' EXHIBIT 142:

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

The State of Missouri,
et al.,

Plaintiffs,

v.

**President Joseph R. Biden, Jr., in his
official capacity as President of the United
States of America,**
et al.,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF LEAH BRAY

I, Leah Bray, declare pursuant to 28 U.S.C. § 1746 the following, based on my personal knowledge and information acquired by me in the course of performing my official duties, and information contained in the records of the Global Engagement Center.

1. I currently serve as a Deputy Coordinator in the Department of State's Global Engagement Center (GEC). I am one of two Deputy Coordinators within the GEC, reporting to the Principal Deputy Coordinator. In this position, I share with senior GEC leadership oversight of the GEC's foreign threat actor and support teams, which focus on countering the primary foreign threat actors in line with the GEC's legislative mandate. I am over the age of 21 years and am competent to make this declaration.
2. In connection with my responsibilities as Deputy Coordinator, I am generally familiar with this civil action.
3. Congress has defined the mission of the GEC as follows: "[t]o direct, lead, synchronize, integrate, and coordinate efforts of the Federal Government to recognize, understand,

expose, and counter foreign state and foreign non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States and United States allies and partner nations.” See National Defense Authorization Act for Fiscal Year 2017, 22 U.S.C. §2656, Pub. L. 114-328, Div. A, Title XII, § 1287, Dec. 23, 2016, 130 Stat. 2546, as amended Pub. L. 115-232, Div. A, Title XII, § 1284, Aug. 13, 2018, 132 Stat. 2076.

4. The GEC carries out its statutory mission to counter propaganda and disinformation from foreign state and foreign non-state actors along five lines of effort: (1) analytics and research, (2) international partnerships, (3) programs and campaigns, (4) exposure, and (5) technology assessment and engagement. In terms of programs and campaigns, the GEC’s Russia, the People’s Republic of China (PRC), Iran, and Counterterrorism teams seek to build societal and institutional resilience to foreign propaganda and disinformation abroad. The GEC produces exposure reports of tactics employed by foreign actors to raise awareness of foreign disinformation and propaganda. The GEC also hosts private sector technology demonstrations, identifies innovative solutions to foreign disinformation and propaganda through overseas technology challenge programs, and engages with social media and technology companies to facilitate a better understanding of the techniques and trends in foreign actors’ dissemination of propaganda and disinformation.
5. Disinformation from foreign state and foreign non-state actors is of critical concern to the United States. For example, disinformation is one of Russia’s most important and far-reaching tools in support of its full-scale invasion of Ukraine. Russia has operationalized the concept of perpetual adversarial competition in the information environment by encouraging the development of a disinformation and propaganda ecosystem. This

ecosystem creates and spreads false narratives to strategically advance Russia's policy goals.

6. Russia creates and spreads disinformation in an attempt to confuse and overwhelm people about Russia's real actions in Ukraine and elsewhere. Russia's intelligence services operate, task, and influence websites that present themselves as news outlets to spread lies and sow discord. Disinformation is a quick and relatively cheap way to destabilize societies and set the stage for potential military action.
7. The GEC plays a key role in coordinating U.S. government efforts and helping to lead a global response to such foreign malign influence. A central part of this effort is exposing foreign state and non-state actors' disinformation tactics so that allied governments and our partners abroad, including civil society organizations, academia, the press, and the international public can conduct further analysis of their own and thereby increase collective resilience to disinformation and propaganda.
8. The scope of this problem is described in the GEC's August 2020 Special Report titled "Pillars of Russia's Disinformation and Propaganda Ecosystem." (Pillars Report) *See* Ex. A. That report explains how "Russia has operationalized the concept of perpetual adversarial competition in the information environment by encouraging the development of a disinformation and propaganda ecosystem that allows for varied and overlapping approaches that reinforce each other even when individual messages within the system appear contradictory." *Id.* at 5. The report explains that Russia's propaganda ecosystem employs "official government statements, state-funded media outlets, proxy websites, bots, false social media personas, cyber-enabled disinformation operations, etc.—and the different tactics these channels use." The report notes that Russia's approach allows it "to

be opportunistic, such as with COVID-19, where it has used the global pandemic as a hook to push longstanding disinformation and propaganda narratives.” *Id.* Organizations identified in the Pillars Report as being involved in the dissemination of foreign propaganda include the Strategic Culture Foundation, Global Research, New Eastern Outlook, News Front, SouthFront, Katchon, and Geopolitica.ru. *Id.* at 12.

9. As just one example, the Pillars Report describes the actions of Global Research, a Canadian website that “has become deeply enmeshed in Russia’s broader disinformation and propaganda ecosystem,” and “serves as a talent pool for Russian and Chinese websites.” *Id.* at 12. According to the Pillars Report, on March 12, 2020, Global Research “attracted widespread attention” when “in two tweets, Chinese Ministry of Foreign Affairs spokesman Zhao Lijan linked to two articles (now removed) which falsely blamed the United States for the COVID-19 outbreak.” *Id.* at 29. The Pillars Report notes that Global Research has sought to frame the COVID-19 pandemic as the product of a Western conspiracy. *Id.*
10. The Pillars Report notes that of the 8,542 articles published by the seven outlets described in paragraph 8, above, between February 1 and April 20, 2020, 1,941 (23%) were shared on Twitter via 20,670 tweets. *Id.* at 64. In addition, between April 1, 2020 and June 30, 2020, the GEC identified 173,000 tweets and retweets that included links to these seven outlets. *Id.* at 65. The Pillars Report observes that “content from these outlets is still shared widely” on Twitter, and approximately 59,000 non-U.S. accounts shared articles from these outlets during the GEC’s reporting period. *Id.*
11. In April 2021, the U.S. Department of the Treasury’s Office of Foreign Assets Control took action against multiple individuals and entities who attempted to disseminate

disinformation and to influence the 2020 U.S. Presidential election at the direction of the Russian Government. The Treasury sanctions included three websites – SouthFront, News Front, and Strategic Culture Foundation – that are affiliated with Russian intelligence services and highlighted in the GEC’s August 2020 Pillars Report. Treasury designated SouthFront and the Strategic Culture Foundation pursuant to E.O. 13848 for having engaged in foreign interference in the U.S. 2020 presidential election. SouthFront was also designated pursuant to E.O. 13694, as amended, and E.O. 13382 for acting on behalf of the Russian intelligence services (the FSB). News Front was designated pursuant to the Countering America’s Adversaries Through Sanctions Act (CAATSA), E.O. 13694, and E.O. 13382 for acting on behalf of the FSB (see <https://home.treasury.gov/news/press-releases/jy0126>).

12. I am aware that plaintiffs in this action have asked for the following preliminary injunctive relief:

The Court should enter a preliminary injunction preventing Defendants, and their agents, officers, employees, contractors and all those acting in concert with them, from taking any steps to demand, urge, encourage, pressure, coerce, deceive, collude with, or otherwise induce any social-media company or platform for online speech, or any employee, officer, or agent of any such company or platform, to censor, suppress, remove, de-platform, suspend, shadow-ban, de-boost, deamplify, issue strikes against, restrict access to, demonetize, or take any similar adverse action against any speaker, content, or viewpoint expressed on social media. The Court should also preliminarily enjoin Defendants from acting in concert with any others, including but not limited to persons and entities associated with the Center for Internet Security, the Election Integrity Partnership, and the Virality Project, to engage in the aforementioned conduct, and from acting in concert with any such others who are engaged in any of the aforementioned conduct.

13. Plaintiffs’ proposed preliminary injunction would significantly harm the GEC’s ability to perform its statutorily mandated work described above of directing, leading, synchronizing, integrating and coordinating the Federal Government’s efforts to recognize,

understand, expose, and counter foreign state and foreign non-state propaganda and disinformation efforts aimed at undermining or influencing the policies, security, or stability of the United States, its allies, and partner nations.

14. For example, under the Plaintiffs' proposed injunction, the GEC would be unable to flag for social media companies examples of propaganda and disinformation by foreign terrorist groups or state actors such as Russia or the PRC aimed at harming U.S. interests.

15. In addition, the GEC would be unable to carry out any parts of its statutory mandate that could result in adverse action by the social media companies against foreign threat actors. For example, under a broad reading of the proposed preliminary injunction, the GEC would be prevented from producing and disseminating reports exposing Russian or PRC malign influence if those reports could be construed as "steps" to "encourage" or "otherwise induce any social-media company" to moderate content in or on their platforms. Such a construction of the proposed injunction could prevent the GEC from exposing foreign malign influence operations such as Russian distortions about the U.S. Biological Threat Reduction Program. Additional examples of GEC publicly available reports exposing foreign malign influence are available at www.state.gov/disarming-disinformation, and below:

- a. **Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War**, February 23, 2023 (describes the evolution of the Kremlin's use of disinformation in the context of the Ukraine war)
- b. **Yevgeniy Prigozhin's Africa-Wide Disinformation Campaign**, November 4, 2022 (describes the role of disinformation in the Kremlin's Africa strategy, including its support to internationally-sanctioned Russian oligarch Yevgeniy Prigozhin and the Wagner Group)
- c. **Fact vs. Fiction: Kremlin Disinformation about International Sanctions**, August 22, 2022 (describes Kremlin disinformation about sanctions applied by the international community related to Ukraine)

- d. **Kremlin-Funded Media: RT and Sputnik's Role in Russia's Disinformation and Propaganda Ecosystem**, January 20, 2022 (describes the role that Russia state-owned and state-directed media play in promoting disinformation globally)
- e. **People's Republic of China (PRC) Efforts to Amplify the Kremlin's Voice on Ukraine**, May 2, 2022 (describes PRC efforts to amplify Kremlin propaganda and disinformation about Ukraine)

16. The GEC's practice is not to request social media companies take any specific actions when sharing information with them. The GEC does not fund programs intended to address disinformation in the United States.
17. In rare instances, the GEC has engaged with a social media company about specific content on the company's platform when circumstances involved potential threats to the safety of State Department personnel. In 2018, for example, a colleague informed Daniel Kimmage, who was then acting Coordinator of the GEC, of a situation abroad in which protestors were using a social media platform to communicate in ways that raised urgent security concerns. Mr. Kimmage subsequently conveyed those concerns to at least one social media platform. The proposed injunction would prevent the GEC from notifying social media companies about online threats to Department personnel overseas and foreign civil society partners.
18. During the 2020 U.S. election cycle, the GEC discovered certain posts and narratives on social media and digital media that originated from, were amplified by, or likely to be amplified by foreign malign influence actors— like Russia, the PRC, Iran and their proxies—that sought to spread propaganda or disinformation about the 2020 election. I have familiarized myself with GEC records about these events, and it is my understanding that the GEC flagged these posts and narratives for the Election Integrity Project (EIP) on approximately 21 occasions. My understanding is that the EIP would then make an

independent determination as to whether to send this information to social media companies, and that the social media companies in turn would make a separate independent decision about what actions, if any, to take based on their own policies and under their respective terms of service with account holders and users of their sites.

19. Presently, the GEC is not doing any work with EIP.

I declare under penalty of perjury that the foregoing is true and correct and that this Declaration was executed in Washington, D.C. on this 27th day of April, 2023.

A handwritten signature in cursive script, reading "Leah Bray".

Leah Bray
Deputy Coordinator
Global Engagement Center
U.S. Department of State

EXHIBIT A



U.S. DEPARTMENT of STATE

GEC Special Report:

**Pillars of Russia's Disinformation and
Propaganda Ecosystem**



August 2020



Table of Contents

Introduction	3
Background	5
The Report	7
Pillars of Russia's Disinformation and Propaganda Ecosystem	8
Pillars of Russia's Disinformation and Propaganda Ecosystem Endnotes	9
Media Multiplier Effect: How Russia's Disinformation and Propaganda Spreads	10
Preface for the Proxy Site Profiles	11
Highlights from the Proxy Site Profiles	12
Proxy Site Profiles	14
The Strategic Culture Foundation	14
New Eastern Outlook	20
Global Research	25
News Front	31
SouthFront	37
Geopolitica.ru	50
Katehon	55
Digital Media Analysis	61
Twitter Analysis	65
References	70

Introduction

Understanding Russia's Disinformation and Propaganda Ecosystem

As the U.S. Government's dedicated center for countering foreign disinformation and propaganda, the Global Engagement Center (GEC) at the U.S. Department of State has a mandate to expose and counter threats from malign actors that utilize these tactics. In this field, Russia continues to be a leading threat. The Department works with interagency and global partners to meet this challenge, with the GEC playing a key role in coordinating efforts and helping lead a global response.

A central part of this effort is exposing Russia's tactics so that partner and allied governments, civil society organizations, academia, the press, and the international public can conduct further analysis of their own and thereby increase collective resilience to disinformation and propaganda.

In line with that goal, this report draws on publicly available reporting to provide an overview of Russia's disinformation and propaganda ecosystem. Russia's disinformation and propaganda ecosystem is the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives. The ecosystem consists of five main pillars: official government communications, state-funded global messaging, cultivation of proxy sources, weaponization of social media, and cyber-enabled disinformation. The Kremlin bears direct responsibility for cultivating these tactics and platforms as part of its approach to using information as a weapon. It invests massively in its

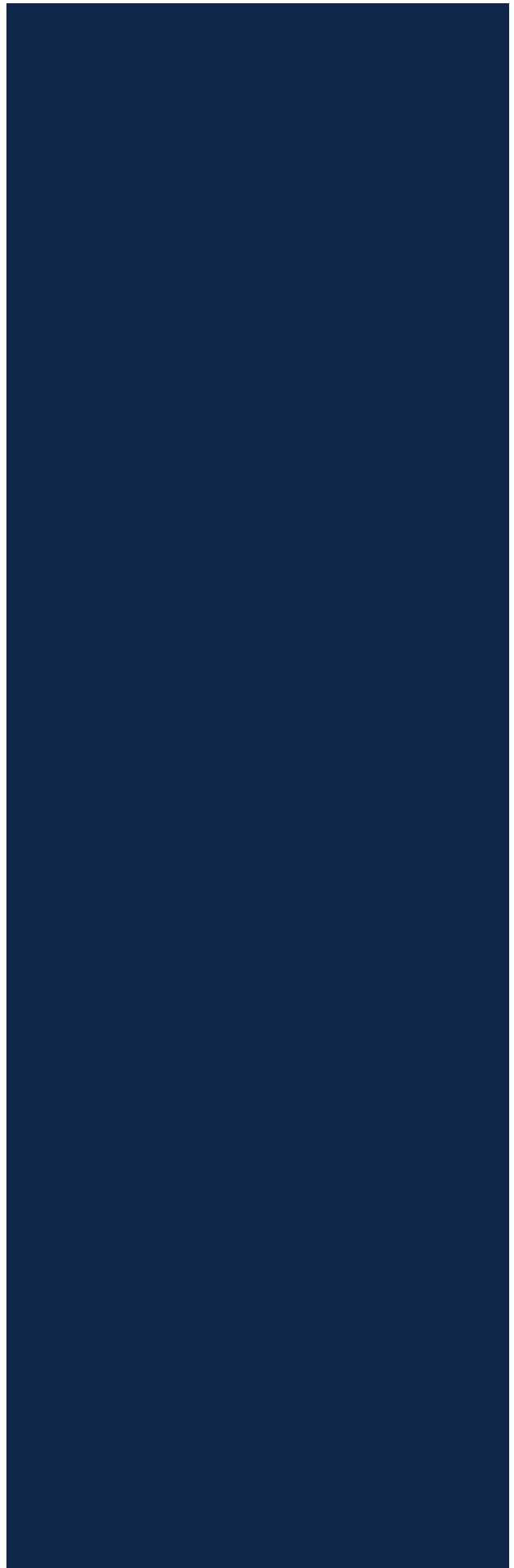
"Russia's disinformation and propaganda ecosystem is the collection of official, proxy, and unattributed communication channels and platforms that Russia uses to create and amplify false narratives."

propaganda channels, its intelligence services and its proxies to conduct malicious cyber activity to support their disinformation efforts, and it leverages outlets that masquerade as news sites or research institutions to spread these false and misleading narratives. This report also focuses specific attention on Russia's tactic of leveraging proxy voices that proliferate pro-Kremlin disinformation and propaganda. It includes profiles on a cross section of outlets playing this role within the broader ecosystem, and it explains how they serve as critical connective tissue to the other pillars within the broader ecosystem.

The GEC has developed the "ecosystem" concept and has broken the ecosystem down into five pillars as a way to contextualize the threat posed by Russia in this field. A common understanding is a necessary prerequisite to developing analytical tools to monitor the various threat vectors and crafting the policies and procedures that allow for countermeasures. While this effort continues, the

issuance of this report aims to heighten awareness of the threat posed by disinformation and further the international dialogue among the nations, organizations, and individuals who are committed to countering these malign efforts.

The disinformation and propaganda ecosystem that Russia continues to cultivate does not stand unopposed. A thriving counter-disinformation community comprised of governments, civil society, academia, the press, the private sector, and citizens around the world who refuse to tolerate these tactics is pushing back. This report is offered by the U.S. Department of State as a contribution to these joint efforts.



Background

In any analysis of Russia's disinformation and propaganda tactics, it is important to note there are multiple terms and concepts that have been used to describe the nature of this threat. "Information Confrontation" is the term used in Russian strategic and military circles to describe their approach to the use of information in both peacetime and conflict. There is also a rich public record of the use of "Active Measures" to describe long-standing Russian political warfare methods that utilize disinformation and propaganda as a core tool. These concepts speak to Russia's strategic formulation that it is in a state of perpetual conflict with its perceived adversaries.

Russia's current disinformation and propaganda operations are an integrated tactical manifestation of this strategic view. Analyzing this approach in a manner that increases resiliency begins with a recognition that there is no single media platform where propaganda and disinformation are distributed. Nor is there uniformity of messages among different sources.

Rather, Russia has operationalized the concept of perpetual adversarial competition in the information environment by encouraging the development of a disinformation and propaganda ecosystem that allows for varied and overlapping approaches that reinforce each other even when individual messages within the system appear contradictory. This ecosystem reflects both the sources of disinformation and propaganda—official government statements, state-funded media

outlets, proxy websites, bots, false social media personas, cyber-enabled disinformation operations, etc.—and the different tactics that these channels use.

Russia's willingness to employ this approach provides it with three perceived advantages. First, it allows for the introduction of numerous variations of the same false narratives. This allows for the different pillars of the ecosystem to fine tune their disinformation narratives to suit different target audiences because there is no need for consistency, as there would be with attributed government communications. Second, it provides plausible deniability for Kremlin officials when proxy sites peddle blatant and dangerous disinformation, allowing them to deflect criticism while still introducing pernicious information. Third, it creates a media multiplier effect among the different pillars of the ecosystem that boost their reach and resonance.

The media multiplier effect can, at times, create disinformation storms with potentially dangerous effects for those Russia perceives as adversaries at the international, national, and local level. In the past, Russia has leveraged this dynamic to shield itself from criticism for its involvement in malign activity. This approach also allows Russia to be opportunistic, such as with COVID-19, where it has used the global pandemic as a hook to push longstanding disinformation and propaganda narratives.

This ecosystem approach is also well-suited to reinforce Russia's general aims of questioning the value of democratic institutions, and of weakening the international credibility and international cohesion of the United States and its allies and partners. Because some pillars of this ecosystem generate their own momentum, as opposed to waiting for specific orders from the Kremlin on every occasion, they can be responsive to distinct policy goals or developing situations, and then pivot back to their status quo of generally pouring scorn on Russia's perceived adversaries.

The perpetual conflict that Russia sees in the information environment also means that officials and state media may take one side of an issue, while outlets with a measure of independence will adopt their own variations on similar overarching false narratives. The ecosystem approach is fitting for this dynamic because it does not require harmonization among the different pillars. By simultaneously furthering multiple versions of a given story, these actors muddy the waters of the information environment in order to confuse those trying to discern the truth.



The Report

This report provides a visual representation of the ecosystem described above, as well as an example of the media multiplier effect it enables. This serves to demonstrate how the different pillars of the ecosystem play distinct roles and feed off of and bolster each other.

The report also includes brief profiles of select proxy sites and organizations that occupy an intermediate role between the pillars of the ecosystem with clear links to Russia and those that are meant to be fully deniable. The emphasis on these proxy sites is meant to highlight the important role they play, which can be overlooked given the attention paid to official Russian voices on one end of the spectrum, and the social media manipulation and cyber-enabled threats on the other.

Disclaimer: The GEC cannot vouch for the security of the sites cited within this report.



PILLARS OF RUSSIA'S DISINFORMATION AND PROPAGANDA ECOSYSTEM



Official Government Communications

- Kremlin or Ministry statement¹
- Official Russian social media post²
- Statement or quote by Russian official³



State-Funded Global Messaging

- State-funded, foreign-facing media⁴
- State-funded, domestic-facing media⁵
- Foreign-based, Russian state-funded media⁶
- International Russian socio-cultural institutions⁷



Cultivation of Proxy Sources

- Russia-aligned outlets with global reach⁸
- Local language-specific outlets⁹
- Witting proliferators of Russian narratives¹⁰
- Unwitting proliferators of Russian narratives¹¹
- Foreign state narrative amplification¹²



Weaponization of Social Media

- Infiltration of domestic conversations¹³
- Standing campaigns to undermine faith in institutions¹⁴
- Amplification of protests or civil discord¹⁵



Cyber-Enabled Disinformation

- Hack & Release¹⁶
- Site capture¹⁷
- Cloned websites¹⁸
- Forgeries¹⁹
- Disruption of official sources or objective media²⁰

CONNECTION TO RUSSIA

← **VISIBLE**

OBSCURED

DENIED →



Global Engagement Center



Endnotes

Official Government Communications

¹Kremlin or Ministry statement

- AP: Russia claims US running secret bio weapons lab in Georgia
- TASS: Neither Soviet Union, nor Russia perform research codenamed Novichok - diplomat
- MFA Russia: Publications in Arab media regarding Russian nationals' involvement in the military operations in Libya
- TASS: Russian Foreign Ministry slams flimsy MH17 accusations of JIT

²Official Russian social media post

- Russian Embassy in UK Twitter: The [Skripal] incident appears to be yet another crooked attempt by the UK authorities to discredit Russia.
- Russian Embassy in Malaysia Facebook.
- Russian Foreign Ministry Facebook: Revisionist History Regarding the Baltic Forest Brothers

³Statement or quote by senior Russian official

- Rossiya 24: MFA Spokeswoman Maria Zakharova claims that Osama bin Laden was welcomed at the White House
- MFA Russia Facebook page: Russian Rep to EU article in the EU Observer citing Dulles Plan

State-Funded Global Messaging

⁴State-funded, foreign-facing media

- Sputnik Mundo: COVID-19 Brings Attention to US Secret Laboratories on the Borders of Russia and China
- Sputnik Czech: COVID-19 mutation may be due to SG
- RT Arabic: Washington accuses Moscow of 'collusion with Assad in support of Haftar'
- RT: Int'l investigators allowed Ukraine to fabricate MH17 evidence - Russia
- Sputnik: Wicked Games: US 'Uses Terrorism as Main Mechanism of Its Foreign Policy'

⁵State-funded, domestic-facing media

- RIA Novosti: Source: Johnson will be put on an artificial lung ventilation machine
- Perviy Kanal: The "Vremya" news program alleged President Trump's connection to COVID-19
- Rossiya 24: Vesti Nedeli, the flagship weekly news analysis program, cited fabricated documents to falsely claim Alexei Navalny was a CIA agent.

⁶Foreign-based, Russian state-funded media

- LINX: The pro-Moscow media (Moldova)
- Coda Story: Russia, The New power in Central Africa (para. 6, 10-11)

⁷International Russian socio-cultural institutions

- Atlantic Council: "The Long Arm of Russian 'Soft' Power"
- Ponsars Eurasia: "Russia's Anti-American Propaganda in the Euromaidan Era"
- The Foreign Policy Centre: "The non-governmental sector: Pro-Russia tools masquerading as independent voices"

Cultivation of Proxy Sources

⁸Russia-aligned outlets with global reach

- Global Research: COVID-19: Further Evidence that the Virus Originated in the U.S.
- Strategic Culture Foundation: The Facts About Crimea Should Be Recognised. And So Should Crimea
- News Front: How karma works: is it possible that COVID-19 is a successful project of the USA?

⁹Local language-specific outlets

- Hlavné Správy (Slovakia): Why They Hate Russia in the West
- Compact Magazine (Germany): Vladimir Putin: Talk to the Germans

¹⁰Witting proliferators of Russian narratives

- The Moscow Times: 'Hybrid Truth': Russia-Linked Italians Sing Praises for Moscow's Virus Aid
- Anton Shekhovtsov: Russia and the Western Far Right: Tango Noir
- Investigation uncovers Dutch politician's ties to Russia

¹¹Unwitting proliferators of Russian narratives

- NATO: The "Lisa Case": Germany as a target of Russian disinformation (last para, 'Russian Networks' section)
- United States Department of Justice: Report On The Investigation Into Russian Interference In The 2016 Presidential Election (pg. 14-15)

¹²Foreign state narrative amplification

- FPRI: Iranian, Chinese and Russian Overt Media on Coronavirus
- EEAS: EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (Update 23 April - 18 May)

Weaponization of Social Media

¹³Infiltration of domestic conversations

- U.S. Senate Select Committee on Intelligence: Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views
- El País: Russian network used Venezuelan accounts to deepen Catalan crisis

¹⁴Standing campaigns to inflame domestic discord & undermine faith in institutions

- International Centre for Defence and Security: Contemporary Deterrence: Lessons and Insights From Enhanced Forward Presence (pg. 12-13)
- Computational Propaganda Project: The IRA, Social Media and Political Polarization in the United States, 2012-2018

¹⁵Russian-instigated or amplified protests

- U.S. Department of Justice: United States v. Internet Research Agency LLC et al. (pgs. 20-23)
- Bloomberg: France to Probe Possible Russian Influence on Yellow Vest Riots

Cyber-Enabled Disinformation

¹⁶Hack & Release

- United States Department of Justice: Report On The Investigation Into Russian Interference In The 2016 Presidential Election (pgs. 38-48)
- Government of the Netherlands: Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW

¹⁷Site Capture

- EU Monitor: "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, (See Annex 18)
- Reuters: Georgia, backed by U.S. and Britain, Blames Russia for 'Paralyzing' Cyber Attack

¹⁸Cloned Websites

- FireEye: APT28: A Window into Russia's Cyber Espionage Operations? (pgs. 11, 13-14)
- New York Times: The Agency (see para. 6; clones of Louisiana news sites)
- Heinrich Böll Stiftung: Finland's Reluctance to Join NATO (see para. 10; clone of Hybrid CoE site)

¹⁹Forgeries

- NPR: Anti-Doping Agency Bans Russia From International Sports Events For 4 Years
- Bellinacat: Comparison of Digital Globe 17 July Satellite Imagery with Russian Ministry of Defense 17 July Satellite Imagery

²⁰Disruption of official sources or objective media

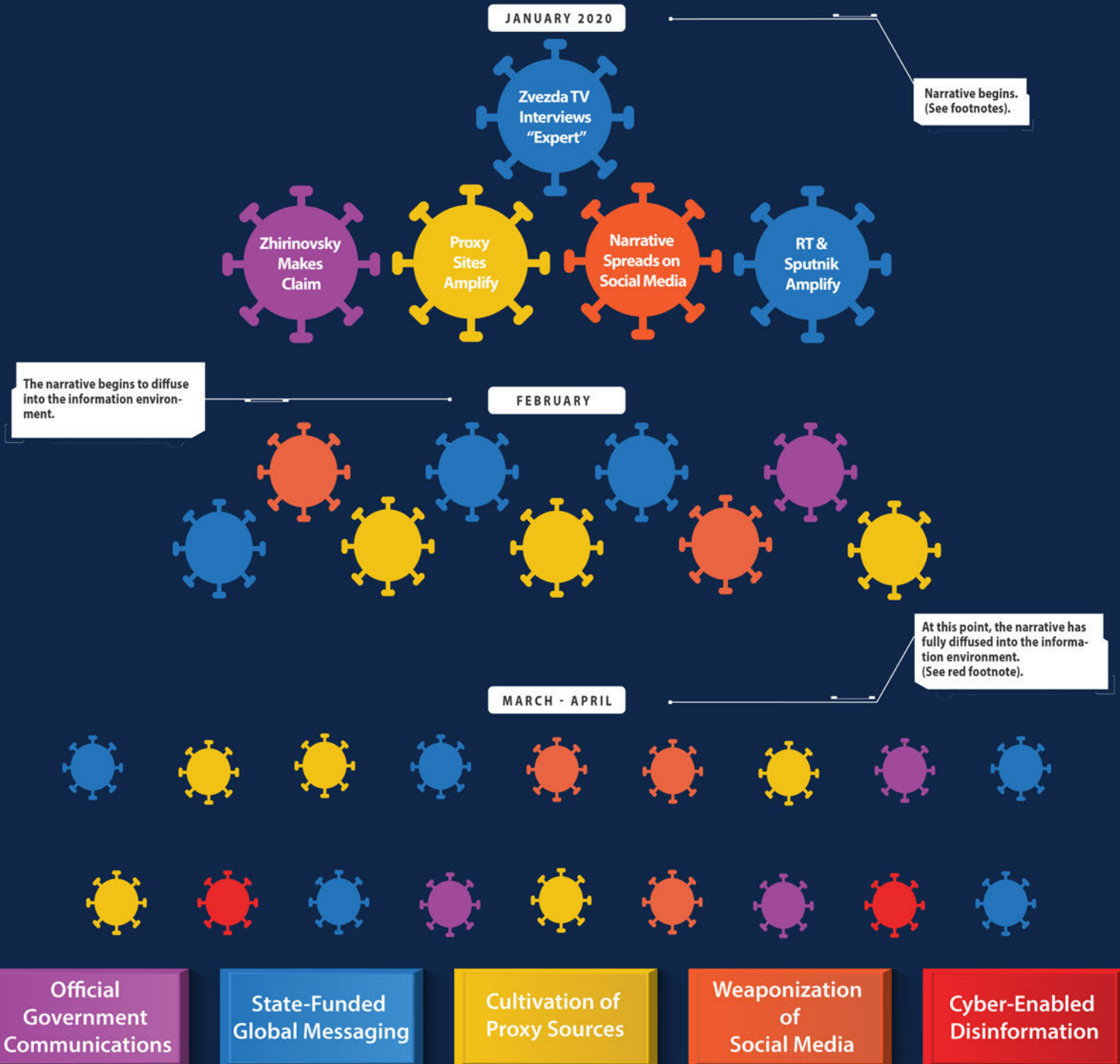
- Reuters: Georgia, backed by U.S. and Britain, Blames Russia for 'Paralyzing' Cyber Attack
- Symantec: WastedLocker: Symantec Identifies Wave of Attacks Against U.S. Organizations

HOW RUSSIA'S DISINFORMATION & PROPAGANDA



SPREADS

The Media Multiplier Effect
False Claim: The U.S. Created COVID-19



Footnotes:

- **Govorit Moskva:** Zhirinovsky calls coronavirus in China a biological weapon of the USA
- **Zvezda TV:** An expert linked an outbreak of pneumonia in China with a biological weapon test
- **Sputnik Arabic:** Is the Coronavirus a secret US biological weapon?
- **Rossiya-1 (60 Minutes):** 60 минут по горячим следам (вечерний выпуск в 17:25) or 24.01.20 (start at 22:30 min)
- **News Front:** The new Chinese virus might be man-made: you need to close the American laboratory in Alma-Ata. "Echo of Kazakhstan"
- **Geopolitica.ru:** Geopolitics of Epidemics: China and SARS Viruses
- **Report: DFRLab:** Bioweapons, secret labs, and the CIA: pro-Kremlin actors blame the U.S. for coronavirus outbreak
- **Report: Mandiant Threat Intelligence - "Ghostwriter" Influence Campaign**

Preface for the Proxy Site Profiles

The following profiles focus on some of the proxy outlets and institutions that proliferate Russia's disinformation and propaganda narratives. As the report notes, some of the individuals and institutions behind these sites benefit greatly from an association with the Kremlin. Others strive to maintain a veneer of separation from Russia, but as our research and analysis show, they serve no other purpose but to push pro-Kremlin content.

The GEC's goal in detailing the nature of these outlets is twofold: to promote a more complete understanding of how these outlets operate as an informal network; and to demonstrate how content produced and amplified by these sites enables the proliferation of disinformation and propaganda across other pillars of the ecosystem.

This collection of profiles is not meant to be exhaustive, nor does it reflect any sort of prioritization or ranking. Rather, it is a select cross section drawn from a multitude of similar operations and is meant to provide a broad representation of the type of outlets that Russia has cultivated to play an important role in its larger disinformation and propaganda ecosystem.

They cover various geographies and have their own target audiences, though there is considerable overlap between some of them largely due to their online presence. While sharing similar practices, they have each developed their own styles. In a few cases, these outlets have published or republished articles authored by false personas attributed by Facebook to Russian military intelligence.

Highlights from the Proxy Site Profiles

The Strategic Culture Foundation

The *Strategic Culture Foundation* is an online journal registered in Russia that is directed by Russia's Foreign Intelligence Service (SVR) and closely affiliated with the Russian Ministry of Foreign Affairs.¹ One of its core tactics is to publish Western fringe thinkers and conspiracy theorists, giving them a broader platform, while trying to obscure the Russian origins of the journal. This tactic helps the site appear to be an organic voice within its target audience of Westerners.

Global Research

Global Research is a Canadian website that has become deeply enmeshed in Russia's broader disinformation and propaganda ecosystem. Its large roster of fringe authors and conspiracy theorists serves as a talent pool for Russian and Chinese websites. Its publications also provide a Western voice that other elements of the ecosystem can leverage to their advantage.

New Eastern Outlook

New Eastern Outlook is a pseudo-academic publication of the Russian Academy of Science's Institute of Oriental Studies that promotes disinformation and propaganda focused primarily on the Middle East, Asia, and Africa. It combines pro-Kremlin views of Russian academics with anti-U.S. views of Western fringe voices and conspiracy theorists. *New Eastern Outlook* appears to want to benefit from the veneer of respectability offered by the Russian academics it features, while also obscuring its links to state-funded institutions.

News Front

News Front is a Crimea-based disinformation and propaganda outlet with the self-proclaimed goal of providing an "alternative source of information" for Western audiences. With reported ties to the Russian security services and Kremlin funding, it is particularly focused on supporting Russia-backed forces in Ukraine. *News Front's* manipulative tactics to boost reach led to a near total dismantling of its presence on social media in early 2020.

Highlights from the Proxy Site Profiles

SouthFront

SouthFront: Analysis and Intelligence

(a.k.a. *SouthFront*), is a multilingual online disinformation site registered in Russia that focuses on military and security issues. With flashy infographics, maps, and videos, *SouthFront* combines Kremlin talking points with detailed knowledge of military systems and ongoing conflicts. It attempts to appeal to military enthusiasts, veterans, and conspiracy theorists, all while going to great lengths to hide its connections to Russia.

Katehon

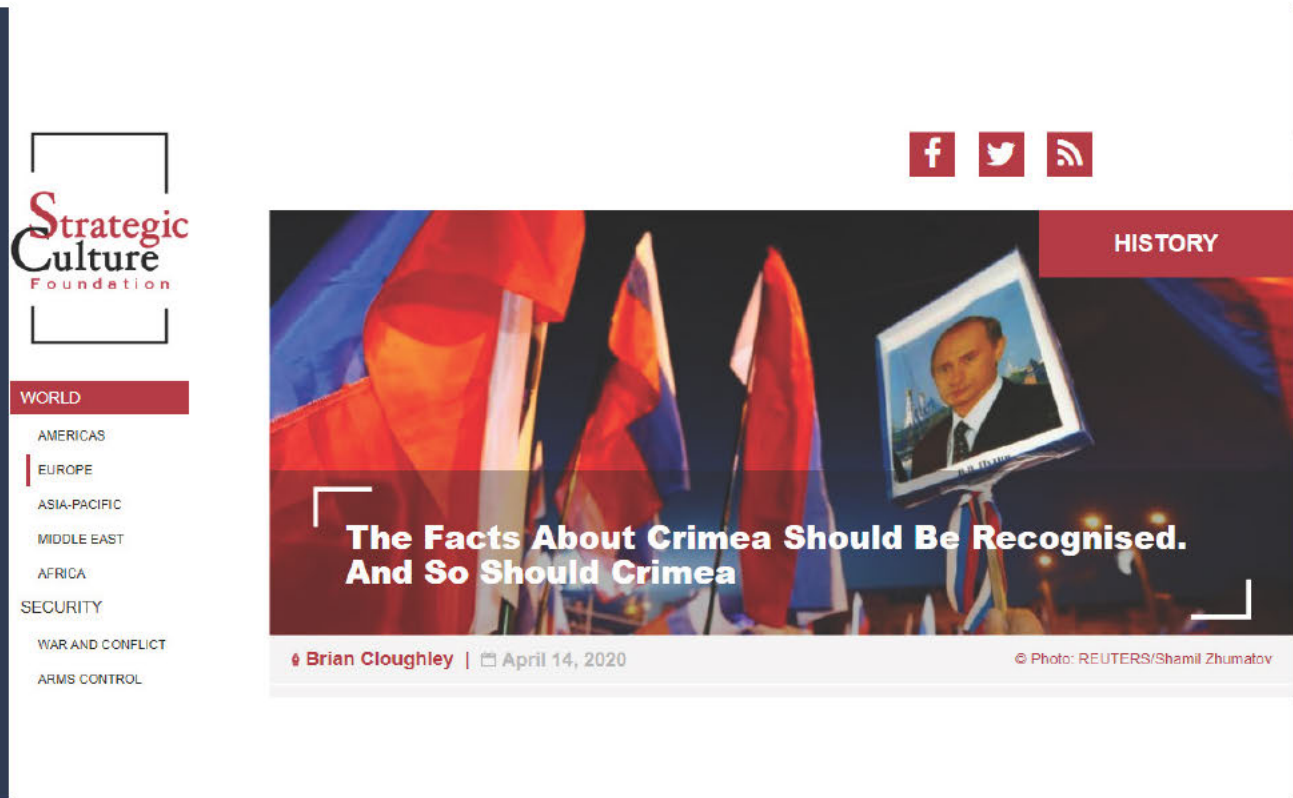
Katehon is a Moscow-based quasi-think-tank that is a proliferator of virulent anti-Western disinformation and propaganda via its website, which is active in five languages. It is led by individuals with clear links to the Russian state and the Russian intelligence services. Within Russia's broader disinformation and propaganda ecosystem, *Katehon* plays the role of providing supposedly independent, analytical material aimed largely at European audiences, with content allegedly dedicated to "the creation and defense of a secure, democratic and just international system".

Geopolitica.ru

Geopolitica.ru serves as a platform for Russian ultra-nationalists to spread disinformation and propaganda targeting Western and other audiences. Inspired by the Eurasianist ideology of the Russian philosopher and Eurasian imperialist Alexander Dugin, *Geopolitica.ru* views itself as caught in a perpetual information war against the Western ideals of democracy and liberalism. The website's cooperation with other outlets in Russia's disinformation and propaganda ecosystem broadens the reach of its messaging, which seeks to destabilize and weaken Western institutions.

Proxy Site Profiles

The Strategic Culture Foundation



An article on Strategic Culture Foundation's website promoting Russia's version of history.

Summary

The *Strategic Culture Foundation* is an online journal registered in Russia, directed by Russia's Foreign Intelligence Service (SVR), and closely affiliated with the Russian Ministry of Foreign Affairs. The outlet plays a central role among a group of linked websites that proliferate Russian disinformation and propaganda.² One of its core tactics is to attract authors who are Western fringe thinkers and conspiracy theorists, giving them a broader platform and obscuring the Russian origins of the journal. This tactic helps the site appear to be an organic voice within its target audience of Westerners.

Introduction

The *Strategic Culture Foundation* (SCF) online journal is a prime example of long-standing Russian tactics to conceal direct state involvement in disinformation and propaganda outlets, and to cultivate local voices to serve as surrogate messengers. SCF finds obscure Western fringe thinkers and conspiracy theorists and gives their typically virulent anti-Western and anti-U.S. views a broad international platform. It does this while giving the misleading impression SCF is independent and unaffiliated with the Russian government.

This approach has several advantages for Russia:

- it gives increased circulation to what would otherwise be fringe voices that suit Russian propaganda goals;
- Russia deflects responsibility by obscuring its sponsorship of the site; and
- the individuals and conspiracy theorists they publish communicate in local idioms and understand their home audiences well.

The *Strategic Culture Foundation* and the Russian State

SCF was [founded](#) in 2005.³ Originally it only published its journal in Russian. In [September](#) 2010, the online journal began to also appear in English.⁴ This marked SCF's debut as an instrument for disinformation and propaganda on the international stage.

While SCF's online journal makes every effort to appear independent, it is directed by Russia's Foreign Intelligence Service (SVR) and closely affiliated with the Russian Ministry of Foreign Affairs.⁵ There is no mention of this affiliation on SCF's English-language [website](#), nor of any link to Russia—including the fact that SCF publishes in Russian.⁶ However, [International Affairs](#), the flagship journal of the Russian Ministry of Foreign Affairs since 1922, [states](#) on its website that SCF is its partner.⁷

SCF's [president](#) is Yuri Prokofiev, who was [Moscow Party Chief](#) from 1989 to 1991 and a Soviet [Politburo Member](#).⁸ Prokofiev is also one of the [founders](#) of the "Russian Organization for Assistance to Special Services and Law Enforcement Authorities" (ROSSPO).⁹ According to its [website](#), ROSSPO works closely with Russian security services to support the policies of the Russian state, facilitate cooperation between state institutions and civil society, and ensure the social protection of the employees of intelligence services and law enforcement authorities.¹⁰

SCF's Director General is Vladimir Maximenko, who is also the director of the no-longer active Russian Unity Foundation, which was focused on [promoting](#) a "positive image of Russia and Russian culture abroad," especially among the so-called Russian compatriots.¹¹

Western Authors on SCF's Website

While SCF made some efforts to attract Western authors when it launched its English-language website in 2010, its writers for years were mostly Russians. This is demonstrated by the preponderance of Russian-authored articles posted on the [2 May 2015 SCF homepage](#).¹² Some examples include:

- Yuri Rubtsov (two articles)
- Pyotr Iskenderov
- Dmitry Minin
- Nil Nikandrov
- Nikolai Bobkin
- Alexander Donetsky (two articles)
- Natalia Meden
- Valentin Katasonov

By comparison, on that same day only three non-Russian authors, including Finian Cunningham and Pepe Escobar, had articles published on SCF homepage. Five years later, the English version of SCF's online journal has undergone a transformation. On the current [SCF homepage](#), the Russian authors have disappeared—replaced by Westerners, although Cunningham and Escobar still remain.¹³

Finian Cunningham, who is originally from Belfast and has a background in agricultural chemistry, is the second-most prolific author for SCF, publishing [more than 550 articles](#) since 2012.¹⁴ In one SCF article, he [refers](#) to the United States as a "lawless rogue state."¹⁵ His other SCF articles include:

- [Give North Korea some respect](#)¹⁶
- [Putin Stands Out as a Real World Leader](#)¹⁷
- [Washington Choreographing All-Out War with Russia?](#)¹⁸
- [The Year US-led Capitalism Became Exposed as Root of Global Conflict](#)¹⁹

Cunningham's work also appears frequently on major Russian state-media outlets [RT](#) (237 results), [Sputnik](#) (330 results), and [RIA Novosti](#) (30 results).²⁰ [Article counts compiled on 9 June 2020.]

Retired Russian Colonel Andrei Akulov is the third most-published author on SCF's English-language website; however, his most recent article is from 2018. Similarly, longtime SCF Russian authors like Dmitry Minin, Valentin Katasonov, Pyotr Iskenderov, and Alexander Mezyaev are still published on the Russian-language website, but they stopped appearing on the English-language website in 2017 or 2018.

Some of the current Western authors on SCF's English site are:

- Brian Cloughley, a former Australian defense attaché in Pakistan who has authored [243 articles](#).²¹ Two of his most recent are: "[The Facts About Crimea Should Be Recognised. And So Should Crimea](#)" and "[Washington Wants an Arctic Circle of Confrontation](#)."²²
- Matthew Ehret, one of the newest Western SCF authors, has written [94 articles](#) since April 2019.²³ He is the founder of the *Canadian Patriot Review* and the [Director](#) of the Rising Tide Foundation.²⁴ Besides being an author for SCF, he also writes for other disinformation sites in Russia's ecosystem, including [Oriental Review](#) and [Geopolitica.ru](#).²⁵ Ehret and the *Canadian Patriot Review* are also ardent advocates of China's Belt and Road Initiative, which they [see](#) as a "force for global progress, poverty eradication, and peace."²⁶
- Cynthia Chung, President of the [Rising Tide Foundation](#), is another new SCF author, writing [15 articles](#) since October 2019. One of her recent articles is "[A 70-Year War on 'Propaganda' Built by the CIA](#)."²⁷

Russian Authors Removed from English-Language Site

SCF has tried to make its English-language site seem entirely disconnected from Russia. As noted above, when it launched its current format in 2010, it combined the writings of Russian academics with Westerners, most of whom were those with fringe views or were conspiracy theorists. The inclusion of Russian academics was likely aimed at giving the online journal the appearance of academic respectability, although most of the Russian academics also took strong anti-Western positions.

For example, a [frequent author](#) through 2018, Moscow State Institute of International Finance professor [Valentin Katasonov](#), wrote an article entitled, "[Anglo-American Money Owners Organized World War II](#)."²⁸ He argued:

The war was not unleashed by frenzied Fuhrer who happened to be ruling Germany at the time. WWII is a project created by world oligarchy or Anglo-American "money owners". Using such instruments as the US Federal Reserve System and the Bank of England they started to prepare for the next world conflict of global scale right after WWI. The USSR was the target.

Another prolific author through 2017 was [Pyotr Iskenderov](#), senior researcher for the Institute for Slavic Studies at the Russian Academy of Sciences.²⁹ Some of his articles included:

- [Modern Nazism as the Driving Force of Euro-Atlantic Integration](#)³⁰

- [The Czech Republic: Doomed without Russia](#)³¹
- [Estonia: Doomed Without Russia](#)³²
- [Russia has enough gas for everyone](#)³³
- [Brussels and Kiev: a duo of blackmailers](#)³⁴

Iskenderov and Katasonov continue to write for the Russian-language version of SCF website, although they disappeared from the English-language version in 2017 and 2018, respectively.

Building a Disinformation Network

In 2010 and 2011, SCF formed explicit partnerships with [Global Research](#), a Canadian website detailed in a separate paper in this report, and [The 4th Media](#), an obscure, newly formed Chinese website in English that described itself as “an independent media organization based in Beijing.”³⁵ Fringe voices and conspiracy theorists that had previously appeared on *Global Research* soon began to be published by SCF and *The 4th Media*, broadening the reach of their anti-Western views.

Cross-Fertilization Within the Network

- *Global Research* has served as a source of “talent” for SCF, *The 4th Media*, and *The 21st Century*. In the first ten years of its operation between 2001 and 2011, *Global Research* developed a large pool of authors from which other websites could draw. The three currently operational websites—SCF, *Global Research*, and *The 21st Century* (a successor website to *The 4th Media*)—appear to have formed a sub-network within the broader array of disinformation and propaganda sites, although their connections have now been obscured.
- SCF: from September 2010 through 8 March 2018, *Global Research* and *The 4th Media* were listed as its partners or at the bottom of its homepage. On 14 March 2018, no websites were listed.
- *Global Research*: From 22 September 2012 through 17 February 2018, its “Partner Websites” included SCF and *The 4th Media*. On 18 February 2018, *The 21st Century* replaced *The 4th Media* on the *Global Research* website as its only opinion website “partner.”
- *The 4th Media*: From 5 August 2011 through 4 March 2019, *Global Research* and SCF were always among the preferred websites listed on its website. Now, *The 21st Century* has no links to other websites.

The reason for this apparently collaborative move to obscure the mutual ties within the network is unclear, but public reporting may have played a role. For further discussion on this topic, see the *Global Research* profile in this report.

Strategic Culture Foundation's Social Media Platforms as of June 2020

Platform	Language	Engagement
Facebook	English	28,182 followers
	Russian	13,187 followers
Twitter	English	dormant since 2019; active once on 8 May 2020
	Russian	218 followers; dormant since 2019
YouTube	English	491 subscribers
VKontakte	Russian	2,590 followers

Proxy Site Profiles

New Eastern Outlook



Screenshot of an article on New Eastern Outlook's website that promotes Russia's version of the Skripal poisoning.

Summary

New Eastern Outlook is a pseudo-academic publication of the Russian Academy of Science's Institute of Oriental Studies that promotes disinformation and propaganda focused primarily on the Middle East, Asia, and Africa. It combines pro-Kremlin views of Russian academics with anti-U.S. views of Western fringe voices and conspiracy theorists. *New Eastern Outlook's* English-language website does not clearly state that it is a product of the Institute. The site appears to want to benefit from the veneer of respectability offered by the Russian academics it features, while also obscuring its links to state-funded institutions.

Introduction



The online journal *New Eastern Outlook* (NEO) first appeared in 2013. Its association with the Russian Academy of Science's Institute of Oriental Studies is not mentioned in NEO's [About Us page](#).³⁶ The logo of the Institute of Oriental Studies with Cyrillic letters (at left) does appear at the bottom of the NEO homepage. It is hyper-linked to the Russian language website of the Institute without any explanation of the connection between the two, even in Russian. The image and link to the website is the only sign of a connection between the organizations visible to visitors of the NEO English language site. Confirmation of the links between them can be found on the Institute's website, where NEO is listed as one of its [periodical publications](#).³⁷

NEO's Partners

NEO lists four "partners" on its [homepage](#).³⁸ None are academic institutions or academics--all are Western conspiracy theorists, fringe groups, or fringe thinkers. One NEO partner has a long history of endorsing bizarre anti-Semitic conspiracy theories while another has written glowingly about North Korea.

NEO's Western Authors

The Western authors published by NEO write highly anti-U.S. anti-Western articles. One such author, Canadian Christopher Black, has written [118 articles](#) for NEO starting in November 2014.³⁹ In February 2020, he [described](#) a U.S. military exercise with NATO allies as a prelude to an attack on Russia, writing:

I have written several times about the continuing NATO preparations for an attack on Russia, a second Operation Barbarossa, the code name for the Nazi invasion of the USSR in 1941. Circumstances prompt me to write about it again, for as of the last week in January the Americans and their gang of lieutenant nations in NATO have commenced the biggest military exercises in 25 years to take place in Europe. The code name for this operation is Defender-Europe 20 but we can interpret that as Attack-Russia 20; in effect a preparation for an attack on Russia comparable to the Nazi invasion in 1941.

Other NEO articles by Black Include:

- [Cuban Resistance: An Example for the World](#)⁴⁰;
- [Paris and Volnovakha: The Brutal Face of Nato Terrorism](#)⁴¹;
- [America Aggression: A Threat To The World](#)⁴²;
- [The Skripal Incident-Another Anti-Russian Provocation](#)⁴³; and
- [War Against Venezuela Is War Against Us All](#).⁴⁴

Another author, Peter Koenig, is a Swiss contributor who has written [52 articles](#) for NEO in the last two years.⁴⁵ On his website, he says that he “writes regularly for *Global Research*; ICH [Information Clearing House]; *RT*; *Sputnik*; *PressTV*; *The 21st Century*; *TeleSUR*; *The Saker Blog*, NEO; and other internet sites.”

In a 28 February NEO [article](#), Koenig advanced conspiracy theories about COVID-19:

With high probability the virus was man-made in one or several bio-warfare laboratories of which the Pentagon and CIA have about 400 around the world . But such high-security bio-labs also exist in Canada, the UK, Israel, and Japan. Western media also are silent about the fact that the virus is directed specifically at the Chinese race, meaning, it targets specifically Chinese DNA.

Almost all the deaths or infected people in the 33 countries and territories to which the virus spread, are of Chinese origin. this is in whatever way you want to turn it, a bio-war against China.⁴⁶

Australian NEO contributor James O'Neill has written [123 articles](#) since 2015.⁴⁷ Five of his first 15 articles were on the topic of the downing of Malaysian Airlines Flight 17 in 2014. In these articles, O'Neill consistently gives credence to Russian denials of involvement while finding fault with the Dutch-led investigation.

O'Neill also writes for the [American Herald Tribune](#), a website that Facebook and Google officials have said is linked to Iranian state media, according to a [CNN article](#).⁴⁸ It disingenuously describes itself as “genuinely independent online media outlet.” *American Herald Tribune* also lists as authors Peter Koenig and other contributors at NEO, as well as and several contributors from the Russian-state-linked [Strategic Culture Foundation](#) (SCF), including Finian Cunningham, Frederico Pieraccini, and Pepe Escobar.⁴⁹

Another frequent NEO author was until recently a member of the tiny, hardline communist Workers World Party (WWP). The WWP was “[created by the KGB](#),” according to Lieutenant General [Ion Mihai Pacepa](#), the former acting head of Romania’s foreign intelligence service in the 1970s.⁵⁰ Pacepa, who defected to the United States in 1978, [writes](#):

The WWP was created by the Soviet KGB in 1957, with the initial task of helping the Kremlin create a favorable impression of the 1956 Soviet invasion of Hungary among the trade unions and “colored” population of the United States. It was run by a Soviet-style secretariat whose members were secretly indoctrinated and trained by the KGB, which also financed its day-to-day operation.⁵¹

The WWP now supports the regimes in [China](#), [North Korea](#), [Cuba](#), and [Russia](#).⁵²

Reprints of NEO Articles

In addition to the *American Herald Tribune*, NEO articles and authors appear in other publications, including:

- *Qoshe*, an online publication that says it seeks to [provide](#) “diverse points of view and opinions” from dozens of worldwide publications.⁵³ [Many](#) are respectable publications but *RT*, *Sputnik*, *TASS*, *PressTV*, and *China Daily* are also included, along with [NEO](#) authors such as Viktor Mikhin.⁵⁴
- [Vijayvaani.com](#), an Indian English-language website that describes itself as “[t]he complete opinions forum.”⁵⁵ It includes articles by:
 - [James O’Neill](#), an author at NEO [since 2015](#), debuting on Vijayvaani.com on 18 May 2020 with the article, “Devastating Revelations About the Truth Behind the Destruction of MH17,” reprinted from [NEO](#).⁵⁶
 - [Viktor Mikhin](#), including his February 28 2020 NEO [article](#) “US Wages Biological Warfare against China.”⁵⁷
 - [Pepe Escobar](#), who writes for SCF.⁵⁸
 - [Israel Shamir](#), “a [Swedish writer and journalist](#), known for promoting antisemitism and Holocaust denial.”⁵⁹
- [New Age](#), which describes itself as “The Outspoken Daily”, is published in Bangladesh. It has published NEO articles by [Yuriy Zinin](#), [Vladimir Terehov](#), [Viktor Mikhin](#), and others.⁶⁰
- *The Fringe News*, which bills itself as “Alternative News Gone Mainstream,” republishes many [NEO articles](#).⁶¹ The site contains no information about who runs it. The “[About Us](#)” section is completely blank. There is also no contact information.⁶²
- [CounterCurrents.org](#), a website in India founded in 2002.⁶³

- *OffGuardian*, which reprints many articles from NEO authors, including 49 by [Christopher Black](#) or mentioning him, and [James O'Neill](#).⁶⁴ The publication takes its name from the fact that “its founders had all been censored on and/or banned from the Guardian’s ‘Comment is Free’ sections.”
- [Veterans Today](#), whose managing editor said NEO has been a “wonderful partner” and described their cooperation as “a marriage made in heaven.”⁶⁵

New Eastern Outlook’s Social Media Platforms as of June 2020

The BBC [reported](#) in July 2019 that NEO’s “Facebook and Twitter accounts have been suspended.”⁶⁶ NEO’s other social media platforms are as follows:

Platform	Language	Engagement
Facebook	English	19,432 likes , account suspended.
YouTube	English	3,150 subscribers; 390,457 total views
GAB	English	45 followers
Pinterest	English	31 followers
Vkontakte	English	575 followers

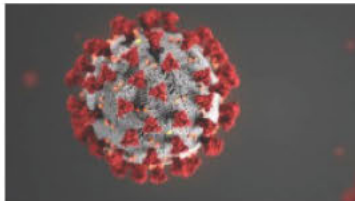
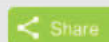
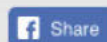
Proxy Site Profiles

Global Research

COVID-19: Further Evidence that the Virus Originated in the US

By [Larry Romanoff](#)
Global Research, March 11, 2020

Region: USA
Theme: Intelligence, Science and Medicine



It would be useful to read this prior article for background:

China's Coronavirus: A Shocking Update. Did The Virus Originate in the US?

By [Larry Romanoff](#), March 04, 2020

Global Research article falsely blaming the United States for creating COVID-19.

Summary

Global Research is a home-grown Canadian website that has become deeply enmeshed in Russia's broader disinformation and propaganda ecosystem. Its large roster of fringe authors and conspiracy theorists serves as a talent pool for the Russian and Chinese websites with which *Global Research* has partnered since the early 2010s. Its publications also provide a Western voice that other elements of the ecosystem can leverage to their advantage.

Introduction

[Global Research](#) is the name of the website of the Centre for Research on Globalization in Canada.⁶⁷ It launched in August 2001 and has been a steady source of anti-U.S. and anti-Western disinformation and propaganda ever since. *The Economist* referred to it as "[a hub for conspiracy theories and fake stories](#)."⁶⁸ Internet watchdog NewsGuard noted, "[t]his website severely violates basic standards of credibility and transparency."⁶⁹

A 2006 article in the *Western Standard* titled "[Canada's Nuttiest Professors](#)" highlighted *Global Research's* head Michel Chossudovsky:

Chossudovsky has manufactured a long list of eyebrow-raising accusations that often read more like wild-eyed conspiracy theories than serious political discourse: the U.S. had foreknowledge of the 9/11 attacks ; “Washington’s New World Order weapons have the ability to trigger climate change”; the U.S. knew in advance about the December 2004 Indian Ocean tsunami, but kept it to themselves (apparently so they could ride to the rescue of devastated coastal regions); big banking orchestrates the collapse of national economies.⁷⁰

As an example of *Global Research*’s work, its [9/11 Reader](#), edited by Chossudovsky, relies heavily on 9/11 “truther” claims, including those of French conspiracy theorist Thierry Meyssan.⁷¹ The French newspaper *Liberation* called Meyssan’s 2002 book [9/11: The Big Lie](#) “a tissue of wild and irresponsible allegations, entirely without foundation.”⁷²

Although the content featured on the site is fringe, *Global Research* has substantial reach. A 2017 [article](#) in Canada’s *The Globe and Mail* noted:

The site has posted more than 40,000 of its own pieces since it was launched in 2001, according to one long-time contributor. But it does more: It picks up reports from other, often obscure websites, thus giving them a *Global Research* link. Those reports often get cross-posted on a series of other sites or aggressively spread across Facebook and Twitter by followers who actively share or retweet them, including a number of social botnets, or bots – automated accounts programmed to spread certain globalresearch.ca content.⁷³

Michel Chossudovsky

Global Research founder and head Michel Chossudovsky is a retired professor who runs the website from his [“upscale condo in Old Montreal.”](#)⁷⁴ Chossudovsky has backed and embraced anti-Western world leaders. In 2004, he volunteered to serve as a [witness](#) for former Yugoslav president Slobodan Milosevic at his trial for war crimes including genocide and crimes against humanity.⁷⁵ In 2011, he and the *Global Research* team extended warm birthday greetings to “Comandante Fidel” Castro of Cuba, saying, “You are the source of tremendous inspiration.” After Chossudovsky met Castro in 2010, he [said](#):

I discovered a man of tremendous integrity, with an acute mind and sense of humor, committed in the minute detail of his speech to social progress and the advancement of humankind .

On a daily basis, Fidel spends several hours reading a large number of detailed international press reports (As he mentioned to me with a smile, “I frequently consult articles from the *Global Research* website”)⁷⁶

Chossudovsky used to be a regular [contributor](#) to the Russian state-funded outlet *RT*, and *Global Research* often [republishes](#) *RT*'s content.

Collaboration with Strategic Culture Foundation, The 4th Media, and SouthFront

Global Research is deeply entwined with other outlets in Russia's disinformation and propaganda ecosystem. As described in the included profile on the *Strategic Culture Foundation* (SCF), *Global Research* has been a partner of SCF since 2011, and with the Chinese website *The 4th Media*, and its successor *The 21st Century* since 2012. In 2012, not long after *The 4th Media* had been formed, Chossudovsky was named as a member of its [international advisory board](#), becoming its [chair](#) in 2015.⁷⁷

Global Research has served as an author talent pool for SCF, *The 4th Media*, and *The 21st Century*. In its first ten years of operation from 2001 to 2011, *Global Research* built a large cadre of authors. Some authors who started off writing for *Global Research* later moved to partner sites. For example, Finian Cunningham wrote [187 articles](#) for *Global Research* from 6 January 2010 to 26 September 2012, close to six articles per month, when he suddenly stopped.⁷⁸ Six weeks later, his [first article](#) for SCF was published, and he resumed this pace of production writing more than [550 articles](#) through May 2020.⁷⁹ Similarly, Pepe Escobar [began writing articles](#) for *Global Research* in 2005 and ten years later became an [SCF author](#).⁸⁰

In addition, *Global Research* also republishes stories from its partner sites. For example, Federico Pieraccini became an [SCF author](#) on 23 July 2016.⁸¹ On the same day, his initial SCF article was [republished](#) by *Global Research*.⁸² About 100 of his SCF articles have since been [republished](#) by *Global Research*.⁸³ In 2016 and 2017, these articles were identified as [originating](#) on SCF.⁸⁴ Beginning in January 2018, however, his *Global Research* articles were [no longer identified](#) as being republished from [SCF](#).⁸⁵

Pieraccini's SCF articles have also appeared on other proxy websites examined in this report, including [SouthFront](#) and [Geopolitica.ru](#), as well in the Russian state-funded outlet [Sputnik](#).⁸⁶ He has also written for [Global Times](#), which is [associated](#) with the Chinese Communist Party's *People's Daily* newspaper.⁸⁷

Global Research frequently publishes articles from other websites in Russia's disinformation and propaganda ecosystem as well. It has published [more than 1 200 articles](#) from *SouthFront*, beginning in April 2015 when *SouthFront* was officially formed. In May 2015, *SouthFront* began to list *Global Research* as one of its [partners](#).⁸⁸

Linkages Among Websites Obscured in 2018

As described in the SCF profile, after 17 February 2018, *Global Research* no longer listed SCF as a partner on its website. At exactly the same time, *The 21st Century*, which revealed no information about its origins, became *Global Research*'s partner, replacing *The 4th Media*, an anti-western blog with alleged links to China. As discussed in the SCF profile, *The 21st Century* is a continuation of *The 4th Media*.

This may have been a collaborative effort by members of the network to obscure their mutual ties. From September 2010 through [8 March 2018](#), SCF listed *Global Research* and *The 4th Media* as partners or featured them prominently at the bottom of its homepage.⁸⁹ On [14 March 2018](#), no websites were listed.⁹⁰

Similarly, on 5 August 2011 and on 4 March 2019, *The 4th Media* listed *Global Research* and SCF as preferred websites on its homepage. However, *The 21st Century*, successor to *The 4th Media*, did not link to other websites. Nevertheless, *Global Research* continued to list *The 21st Century* as a partner, indicating they maintained ties. Similarly, as discussed above, in January 2018 *Global Research* began to omit the fact that its articles by Federico Pieraccini originated from SCF, although they had acknowledged this before.

As noted in the profile of SCF, the reason for the apparently collaborative move to obscure the mutual ties within the network is unclear. However, two media articles looking into the links among the websites in November 2017 may have played a role.

In November 2017, Canada's *The Globe and Mail* asked *Global Research* head Michel Chossudovsky about its ties with Russia and Syria. They [reported](#):

Mr. Chossudovsky didn't want to discuss that. He declined to speak about how globalresearch.ca functions and whether it is aligned with Moscow or any other government.⁹¹

After the newspaper questioned Chossudovsky further:

Mr. Chossudovsky responded through a lawyer, Daniel Lévesque. In a letter, Mr. Lévesque said the Centre for Research on Globalization denies that it is part of a network of pro-Russia or pro-Assad sites or that it is "affiliated with governmental organizations or benefits from their support."

Just eight days after *The Globe and Mail* article was published, the Atlantic Council's Digital Forensic Research Lab (DFRLab) ran an [article on](#) *The 4th Media*, noting its ties with SCF and *Global Research*. It stated:

[The] 4th Media is advertised on the website of a Moscow-based Strategic Culture Foundation (SCF). The advertisement features the logo of The 4th Media at the bottom of the site, along with the logo of GlobalResearch.ca, a media outlet which [@DFRLab](#) repeatedly reported on and remains involved in spreading pro-Kremlin disinformation.

Similarly, at the bottom of The 4th Media website, several logos are featured including state-sponsored media outlets, whose messaging routinely matches that of the governments which fund them, as well as the Moscow-based SCF.

there is no publicly available information about the relationship between The 4th Media and SCF. However, The 4th Media reposts a significant amount of content verbatim from SCF.⁹²

Disinformation on COVID-19

Global Research attracted widespread attention on 12 March 2020 when in [two tweets](#), Chinese Ministry of Foreign Affairs spokesman Zhao Lijian linked to two articles (now removed) which falsely blamed the United States for the COVID-19 outbreak.⁹³ Given *Global Research's* longstanding, openly proclaimed partnership with Chinese websites, it is perhaps no accident that two of their articles were selected by the Foreign Ministry spokesperson.

The author of the two articles, Lawrence Devlin (Larry) Romanoff, identified as a [Canadian writer](#), has pushed false narratives about alleged U.S. bioweapons previously, along with strongly anti-Western views.⁹⁴ In his *Global Research* article "[Understanding China](#)" he claimed, "Westerners live in an illusionary black and white world framed for them by the programming from their Zionist media."⁹⁵ He includes Japan as part of what he calls the "Zionist West." Romanoff lives in Shanghai and says he is "writing a series of ten books generally related to China and the West."⁹⁶

Global Research reacted to the appearance of COVID-19 by seeking to frame it as a Western conspiracy. Between 1 March and 10 April 2020, the most popular *Global Research* articles posted on their Twitter account, [@CRG_CRM](#), speculated that the virus originated in the United States and that COVID-19 was engineered by the global elite to take control of the world.⁹⁷

Chossudovsky has also written many articles on COVID-19. One of them is "[COVID-19 Coronavirus: A Fake Pandemic? Who's Behind It? Global Economic Social and Geopolitical Destabilization](#)," published on the *Global Research* site on 1 March 2020.⁹⁸ This article was republished or linked to by at least 70 different websites and publications, including:

- [Econews Portal](#)¹⁹⁹
- [Jamaica Peace Council](#)¹⁰⁰
- [Tlaxcala](#)¹⁰¹
- [The Real Truth Blog](#)¹⁰²
- [Australian National Review](#)¹⁰³
- [SouthFront](#)¹⁰⁴

GRU Authors

Global Research published or republished seven authors attributed by Facebook to be false online personas created by The Main Directorate of the General Staff of the Armed Forces of the Russian Federation, popularly known as the GRU. Sophie Mangal, Anna Jaunger, Milko Pejovic, Adomas Abromaitis, Mariam al-Hijab, Said al-Khalaki and Mehmet Ersoy were identified by Facebook as false online personas created by the GRU, as noted in [Potemkin Pages & Personas: Assessing GRU Online Operations 2014-2019](#) by Renee DiResta and Shelby Grossman, published by the Stanford Internet Observatory in November 2019.¹⁰⁵ Altogether, these seven GRU personas are responsible for 108 articles that appear on Global Research's website.

Global Research's Social Media Platforms as of June 2020

Platform	Language	Engagement
Facebook	English	279,291 followers
Twitter	English	37,300 followers
YouTube	English	35,800 subscribers, 4,683,769 views

Proxy Site Profiles

News Front

How karma works: is it possible that COVID-19 is a successful project of the USA?

30.03.2020 19:27

Share  388    

According to the WHO report on the spread of the new coronavirus pneumonia, as of March 30, 2020, 717 992 infection cases were confirmed worldwide, 150 914 patients recovered, 33 883 cases were fatal.



Screenshot of a News Front article falsely claiming that the U.S. could have created COVID-19.

Summary

News Front is a Crimea-based disinformation and propaganda outlet with the self-proclaimed goal of providing an “alternative source of information” for Western audiences, a branding technique common among actors in Russia’s disinformation and propaganda ecosystem. With reported ties to the Russian security services and Kremlin funding, it is particularly focused on supporting Russian proxies in Ukraine. *News Front* is one of the most blatant Russian disinformation sites, and its manipulative tactics to boost reach led to a near total dismantling of its presence on social media in early 2020.

Introduction – On the Information Front Against Ukraine

The Crimea-based *News Front* information agency was [registered](#) with Roskomnadzor, the Russian state agency that oversees mass media, in June 2015.¹⁰⁶ *News Front*’s parent company is [Media Group News Front](#), co-founded by Konstantin Knyrik, the [head](#) of *News Front*.¹⁰⁷ According to Knyrik, *News Front* was [originally](#) called *Crimean Front*, and was established to provide informational support for Russia’s attempted annexation of the Ukrainian peninsula.¹⁰⁸ Following the events of 2014, *Crimean Front* became *South-Eastern Front* and eventually evolved into *News Front*.

News Front operates a multi-lingual [website](#), publishing content in Slovak, Georgian, Hungarian, French, Serbian, Spanish, German, Bulgarian, English, and Russian and [claiming](#) to have editorial branches in Bulgaria, Serbia, Germany, France, the UK, Georgia, and Hungary.¹⁰⁹ According to a 2018 article in [Coda](#), *News Front* had ten employees and at least 100 contributors around the world.¹¹⁰

News Front's sources of funding remain opaque. Knyrik [claimed](#) that his organization was financed solely through “donations from his family, friends and income from other business activities,” but a former *News Front* staffer [told](#) German publication *Zeit* that Russian security services allocate funding that makes up “a large part of the budget.”¹¹¹ The Russian independent media outlet *Znak* reported that in 2016, Global Information Technologies, a civil society group [founded](#) by Knyrik and *News Front's* chief anchor Sergey Veselovskiy, [received](#) a 3 million ruble (approximately \$43,070) Presidential Grant to finance *News Front*.¹¹² Media Group News Front and Global Information Technologies are registered at the same address.

Time magazine [questioned](#) Knyrik's self-proclaimed independence from “government influence,” pointing out that *News Front* reporters have “been granted extraordinary access” to the Russian military and are often embedded “with Russian troops and paramilitaries fighting in Syria and eastern Ukraine.”¹¹³ According to [documents](#) from Crimea occupation authority-owned V.I. Vernadsky Crimean Federal University, Media Group News Front is on its list of potential employee options for students graduating in computer science.¹¹⁴

Disinformation and Social Media Manipulation

News Front [purports](#) to provide “objective coverage,” while Knyrik [views](#) the outlet as a “volunteer participant” in the information war against the West, [claiming](#) that *News Front* serves as “an alternative source of information for people in Europe and the U.S.”¹¹⁵ Various media outlets, however, have described *News Front* as leading “[the most aggressive information war against Ukraine](#)” following a “[staunchly pro-Kremlin line](#),” “rarely even” pretending to “[uphold traditional journalistic standards](#),” and [inventing](#) most of its content.¹¹⁶ The Atlantic Council's DFRLab [noted](#) *News Front's* use of photoshopped content.¹¹⁷ A former *News Front* employee [told](#) *Zeit* that “certain topics [for *News Front's* content are] assigned directly from the [Russian] presidential administration.”¹¹⁸

The EU's counter-disinformation product EUvsDisinfo has [documented](#) numerous examples of disinformation and propaganda published on *News Front's* multi-lingual website.¹¹⁹ Recent false narratives include:

- The United States [created](#) the coronavirus as a bioweapon, tested deadly viruses on humans in [Ukraine](#) and China, developed [bacteriological](#) weapons specifically aimed at certain [ethnic](#) groups, intentionally infected [U.S.-based migrants](#) with COVID-19, and [transported](#) the virus to China.¹²⁰

- Cooperation with Europe is a [catastrophe](#) for Ukraine. Ukraine has become a [colony of the IMF and George Soros](#), and its president is a [CIA puppet](#). Ukraine cannot control the coronavirus, as more than 1,500 [Ukrainian soldiers](#) in Donbas are infected with COVID-19. Nazis are [patrolling](#) Kyiv's streets, and a Ukrainian army [veteran](#) drove a truck into demonstrators in Minneapolis.¹²¹
- The EU is [dead](#), it cannot handle the COVID-19 pandemic, and has [abandoned](#) Ukraine. The EU is [inflaming](#) the war in Donbas and is attempting to [destabilize](#) Belarus.¹²²



A screenshot of a post from the suspended News Front's Facebook page.

- NATO did not [provide](#) any COVID-19 assistance to Spain, [does not care](#) about Montenegro, and [spreads](#) the coronavirus in the EU.¹²³
- Bill Gates is [linked](#) to the COVID-19 outbreak and uses the pandemic to implant [microchips](#) "in whole of humanity [sic]." COVID-19 [vaccines](#) are a fraud spearheaded by Gates and Big Pharma.¹²⁴

In April 2020, Facebook [removed](#) a network of accounts, including accounts associated with *News Front*, for "violating [Facebook's] policy against foreign interference which is coordinated inauthentic behavior on behalf of a foreign entity."¹²⁵ The network posted content in Russian, English, German, Spanish, French, Hungarian, Serbian, Georgian, Indonesian, and Farsi on "topics such as the military conflict in Ukraine, the Syrian civil war, the annexation of Crimea, NATO, US elections, and more recently the coronavirus pandemic." Facebook stated that "the individuals behind this activity relied on a combination of authentic, duplicate and fake accounts posing as independent news entities in the regions they targeted."¹²⁶ In addition to *News Front*, Facebook linked the network's "coordinated inauthentic behavior" to another Kremlin-aligned disinformation outlet, *SouthFront*, which according to Facebook is also based in Crimea.¹²⁷ (For more information on *SouthFront* and its connections to *News Front*, see the *SouthFront* profile in this report).

News Front's YouTube Takedown Elicits Response from Russian MFA

On 20 May 2020, Knyrik [announced](#) on his Facebook page that *News Front's* channels had been removed from YouTube.¹²⁸ As of 7 April, *News Front's* YouTube channels collectively had more than 484,000 subscribers and 479,591,989 total views. According to [YouTube](#), the channels were "terminated for a violation of YouTube's Terms of Service."¹²⁹ Following the termination, the Russian Ministry of Foreign Affairs

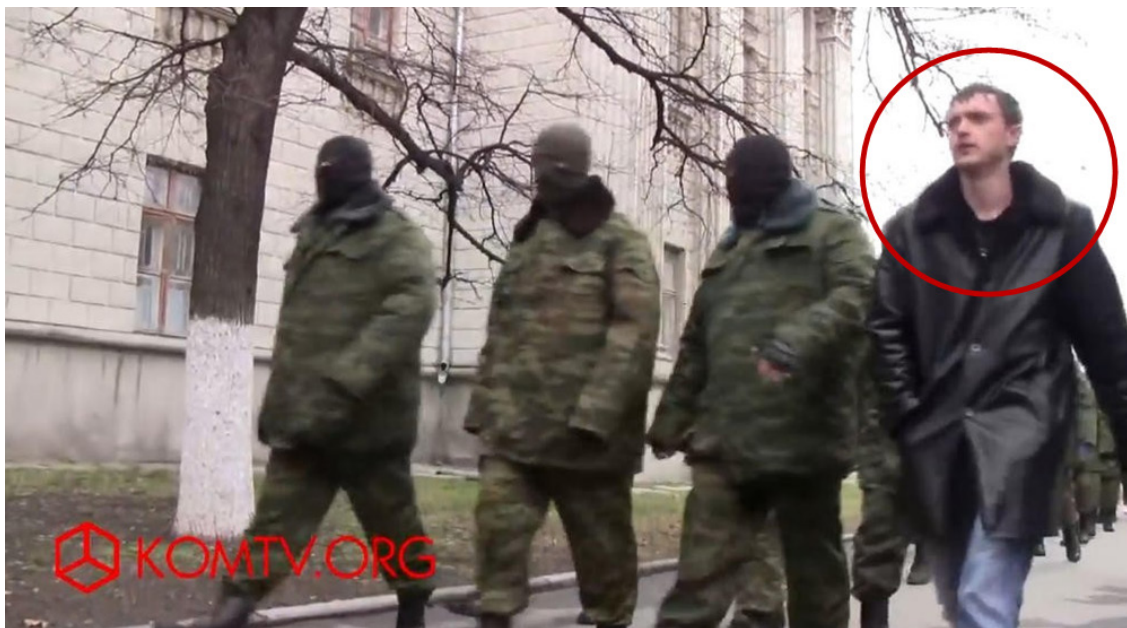
(MFA) issued a [statement](#) condemning YouTube's decision.¹³⁰ Twitter also [suspended](#) *News Front's* accounts for violating "the Twitter Rules."¹³¹

DFRLab, which [analyzed](#) Facebook's takedown of pages and accounts affiliated with *News Front*, found that the agency's Spanish-language pages heavily amplified content from Russian state-controlled media outlets *RT*, *Sputnik*, *TASS*, and *RIA Novosti*. According to DFRLab, the fourth-most amplified source on *News Front's* Spanish-language web page between December 2019 and April 2020 was the Kremlin-aligned disinformation outlet *SouthFront*.¹³²

The International Society for Fair Elections and Democracy (ISFED), a Georgian civil society group, [concluded](#) that *News Front's* Facebook activity in the country included theft of platform users' identities. It detailed *News Front's* efforts "instigating antagonism and aggression among Georgian Facebook users, dividing the society...creating political polarization" and "employing a range of tactics to spread anti-Western, pro-Russian messages."¹³³

***News Front* Leadership: Ties to Russia-Backed Proxies in Ukraine and Russian Ultra-Nationalists**

News Front previously [stated](#) that Knyrik was directly involved in the Russian operation to seize Crimea in violation of international law, including the organization of the illegitimate 2014 referendum. For his actions, he was reportedly awarded a medal from the Russian Ministry of Defense.¹³⁴ The security services of the self-proclaimed Russia-backed "Luhansk People's Republic" (LPR) [awarded](#) Knyrik a medal for cooperation.¹³⁵ In a [video](#) published in 2014, *News Front* anchor Veselovskiy claimed that Knyrik was fighting on the front lines in the so-called LPR.¹³⁶ Knyrik is [reportedly](#) banned from entering Germany for "working for the Russia-supported rebels in eastern Ukraine."¹³⁷



Konstantin Knyrik leads the takeover of the Crimean Center for Investigative Reporting.

In March 2014, Knyrik [reportedly](#) led a raid of Russia's proxy fighters in Crimea to take over the office of the "the region's leading independent news source, the Crimean Center For Investigative Reporting," declaring that the building will now serve as the new headquarters of *Crimean Front*.¹³⁸

Anton Shekhovtsov, a scholar of Russian and European far-right movements, [documented](#) Knyrik's ties to Russian philosopher and ultra-nationalist Alexander Dugin and the Eurasian Youth Union, both [sanctioned](#) by the United States for "actively" recruiting "individuals with military and combat experience to fight on behalf of the self-proclaimed [Donetsk People's Republic] DPR."¹³⁹ (For more information on Dugin see the *Geopolitica.ru* and *Katehon* profiles in this report). In a 2014 interview, Dugin [said](#) he had known Knyrik for more than ten years, describing him as a hero, the "vanguard of the Russian spring in Crimea," and an advocate for the inclusion of Ukraine into the "united Russian world."¹⁴⁰ Knyrik [stated](#) that his priority was to "focus on the creation of the empire; the first goal is to break Crimea away from Ukraine. To join it to the empire first."¹⁴¹

Knyrik and other *News Front* leaders, including its General Director [Yuriy Fedin](#) and chief anchor [Sergei Veselovsky](#), are [affiliated](#) with the Russian ultra-nationalist [Rodina party](#), founded by the [U.S.-sanctioned](#) Russian politician Dmitriy Rogozin.¹⁴² Knyrik is the Committee Chairman of Rodina's regional branch. Sergei Veselovsky is the branch's Deputy Chairman. Yuriy Fedin ran on behalf of Rodina in local elections. Knyrik's [page](#) on the Russian social media platform VKontakte features many photographs of Knyrik and another [U.S.-sanctioned](#) Russian [politician connected to Rodina](#), Sergey Glazyev, former advisor to President Putin¹⁴³ (For more information on Glazyev, see the *Katehon* profiles in this report.) *News Front's* [co-founder](#) Mikhail Sinelin is Glazyev's brother-in-law, [according](#) to the Russian business daily *Kommersant*.¹⁴⁴ RFE/RL [reported](#) that Sinelin was a former deputy chairman of the Russian state-owned bank Vnesheconombank, and worked for about ten years in the secretariats of the Russian vice prime minister and prime minister.¹⁴⁵

News Front's Social Media Platforms as of June 2020:

Platform	Language	Engagement
VK	English	1,140 members
	French	1,248 followers
	Bulgarian	1,200 members
	Russian	149,089 members
	German	1,739 members
	Serbian	1,091 members
	Spanish	1,619 members
Facebook	Russian	111 members
	French	621 followers
	French	516 followers
	English	Account suspended
	Georgian	Account suspended
	Spanish	Account suspended
	German	Account suspended
	Bulgarian	Account suspended
	Serbian	Account suspended
Twitter	English	All accounts suspended
	Bulgarian	
	Russian	
	German	
	Serbian	
	Spanish	
YouTube	English	Account suspended
	Russian	7.74K subscribers, last updated 3 years
	Russian	1.63K subscribers, last updated 4 years ago
	German	Account suspended
	International	Account suspended
	Bulgarian	Account suspended
	Serbian	Account suspended
	Spanish	Account suspended
Odnoklassniki	Russian	14,282 members
Telegram	Russian	9,995 members

Proxy Site Profiles

SouthFront



Screenshot of the SouthFront logo.

Summary

SouthFront: Analysis and Intelligence (a.k.a. *SouthFront*), is a multilingual online disinformation site registered in Russia that focuses on military and security issues. With flashy infographics, maps, and videos, *SouthFront* combines Kremlin talking points with detailed knowledge of military systems and ongoing conflicts. It attempts to appeal to military enthusiasts, veterans, and conspiracy theorists, all while going to great lengths to hide its connections to Russia. Evidence indicates that *SouthFront* has connections to *News Front*, another disinformation and propaganda outlet detailed in this report.

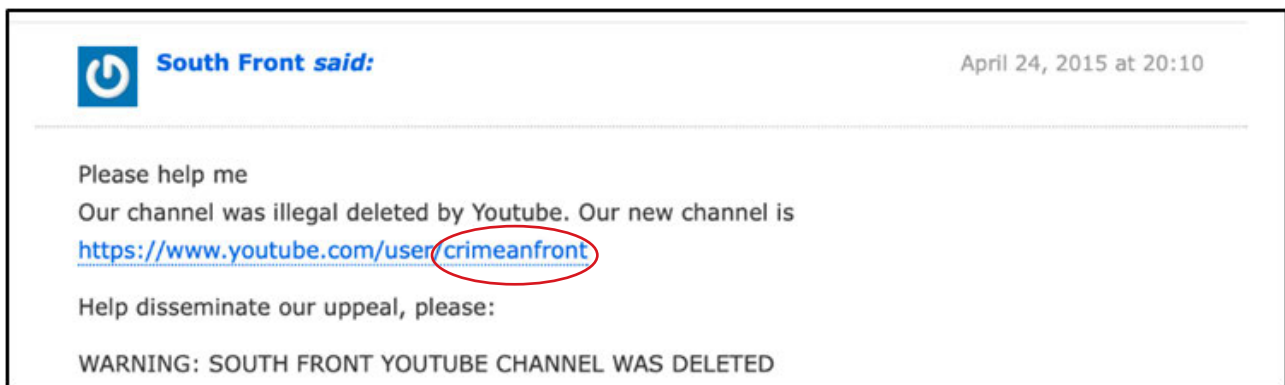
Introduction - Origins

SouthFront: Analysis and Intelligence was first [registered](#) as a formal organization to the domain registration site Reg.ru on 30 April 2015 in Moscow.¹⁴⁶ Currently, *SouthFront* is hosted in Amsterdam by KoDDoS, a Hong Kong-based offshore website hosting and anti-DDoS company.¹⁴⁷ Its content is currently available in English, Russian, and German, with the website previously featuring content in Arabic, Czech, French, and Farsi at various periods in its history.

Facebook accounts associated with *SouthFront* were [removed](#) by the platform in April 2020 for “violating [Facebook’s] policy against foreign interference which is coordinated inauthentic behavior on behalf of a foreign entity.”¹⁴⁸ The network posted content on “topics such as the military conflict in Ukraine, the Syrian civil war, the annexation of Crimea, NATO, US elections, and more recently the coronavirus pandemic” in Russian, English, German, Spanish, French, Hungarian, Serbian, Georgian, Indonesian, and Farsi. Facebook [stated](#) that “the individuals behind this activity relied on a combination of authentic, duplicate and fake accounts posing as independent news entities in the regions they targeted.”¹⁴⁹

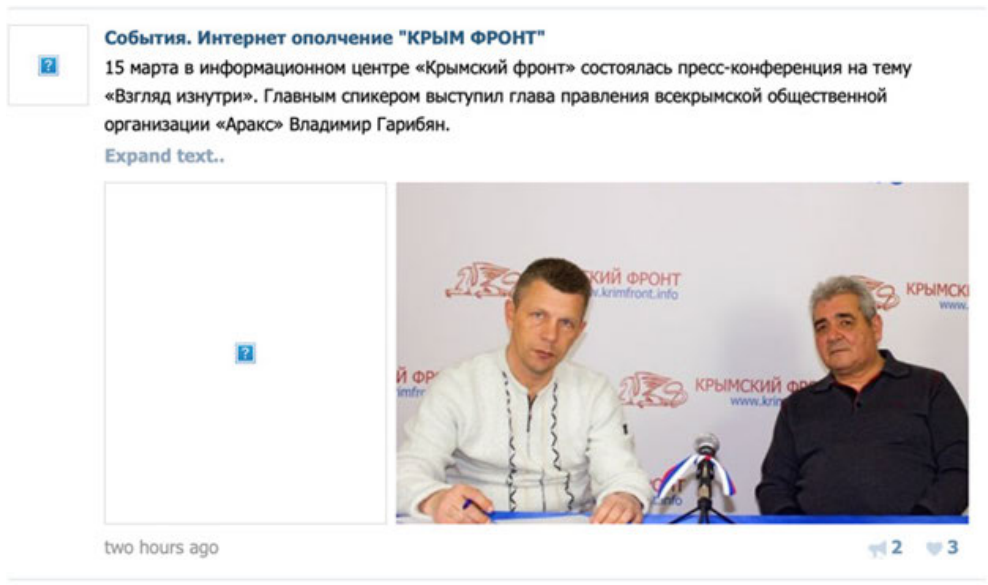
In addition to *SouthFront*, which Facebook claimed was based in Crimea, the company linked the network’s “coordinated inauthentic behavior” to *News Front*, another Kremlin-aligned Crimea-based disinformation outlet covered in this report. While *SouthFront* [claimed](#) that it “has no connection to *News Front* nor operations in Crimea,” there are multiple indications to the contrary.¹⁵⁰ In fact, evidence indicates that *News Front* and *SouthFront* at least began as sister organizations.

According to *News Front*’s founder and leader Konstantin Knyrik, *News Front* was [originally](#) called *Crimean Front* and was established to provide informational support for the Russian attempted annexation of Crimea.¹⁵¹ After 2014, *Crimean Front* became *South-Eastern Front* and then evolved into *News Front*. In a 2015 [online correspondence](#) with one of its initial official partners, the now defunct pro-Russian, pro-Assad disinformation outlet *Syrian Free Press*, *SouthFront* claimed that YouTube removed its channel named *Crimean Front*.¹⁵²

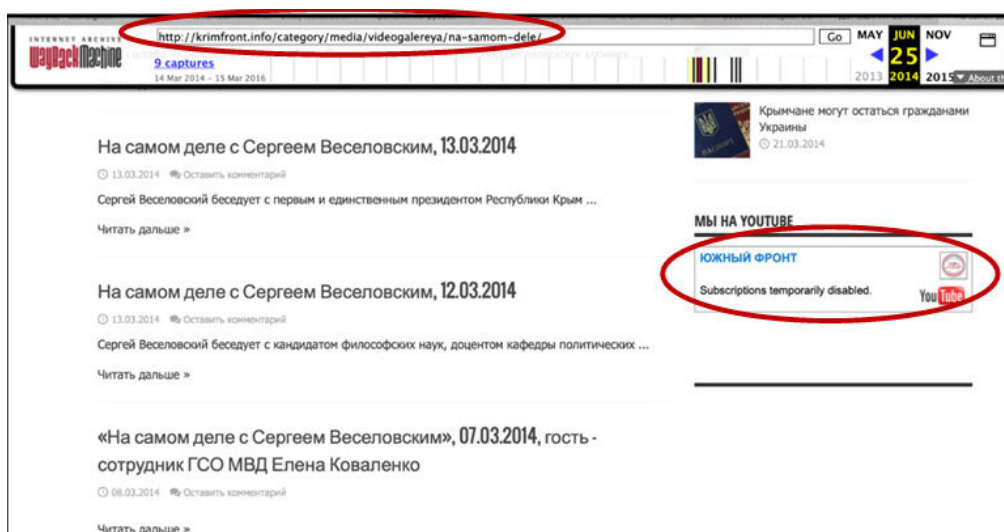


Screenshot of a 2015 online correspondence between SouthFront and Syrian Free Press.

An archived 2014 page of the *Crimean Front* YouTube channel (Крымский Фронт) includes several [links](#) to its affiliated pages on other social media platforms, including a [page](#) on the Russian platform VKontakte titled “События. Интернет ополчение ‘КРЫМ ФРОНТ’” (“Events. Internet militia ‘Crimea Front’”).¹⁵³ The page features several photographs of Sergei Veselovskiy, *News Front*’s current chief anchor, suggesting that he was affiliated with *Crimean Front*. An archived [page](#) from *Crimean Front*’s website showcases Veselovskiy’s program and promotes a YouTube channel named Южный Фронт (Southern Front) under the headline “We are on YouTube.”¹⁵⁴



Screenshot of a post from the "Events. Internet militia 'Crimea Front'" archived VKontakte page featuring Veselovskiy (on the left).



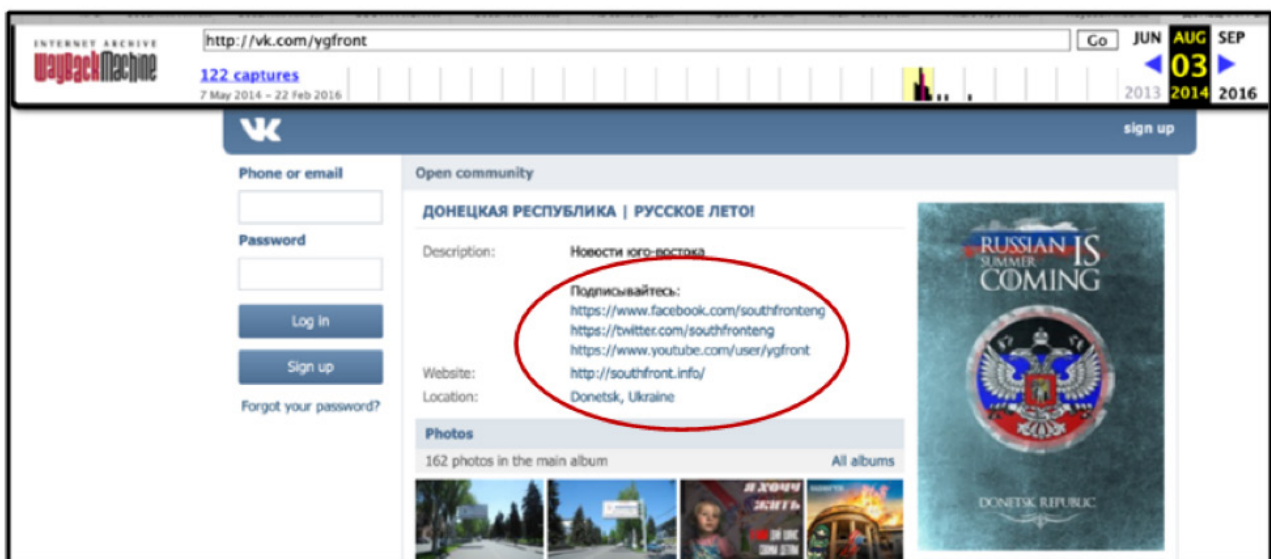
Screenshot of the Crimea Front website featuring Veselovskiy's program and linking to SouthFront's YouTube channel.

An archived 2014 VKontakte post from *Crimean Front* promoted a [post](#) from another VKontakte page titled Южный Фронт (Southern Front), announcing the creation of a new "internet-militia" called *Southern Front*.¹⁵⁵ According to the post, *Crimean Front's* "principles and ideas" served as the "ideological and spiritual platform for the warriors of *Southern Front*."



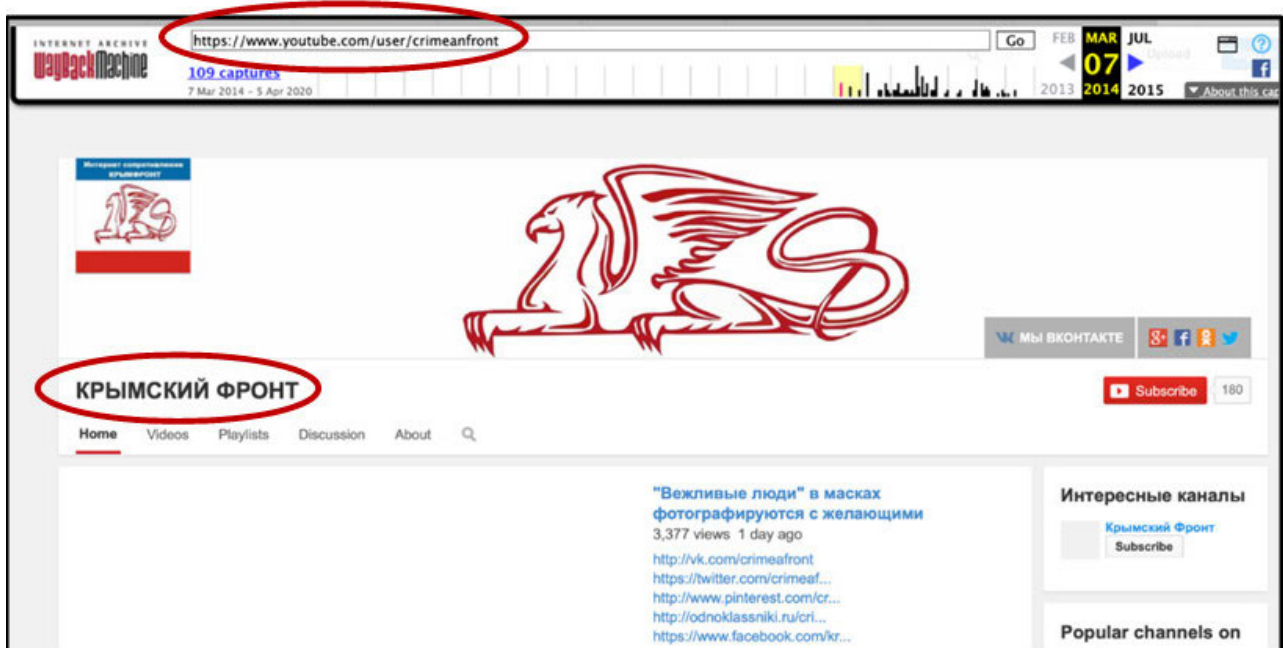
Screenshot (translated on the right) from the archived Crimean Front VKontakte page announcing the creation of the "Internet-militia 'Southern Front'".

Southern Front's archived VKontakte [page](#) titled Донецкая Республика | Русское лето! (Donetsk Republic. A Russian summer!) lists its location as Donetsk, Ukraine and links to several social media accounts, including a [Twitter account](#) still administered today by *SouthFront* (see below).¹⁵⁶

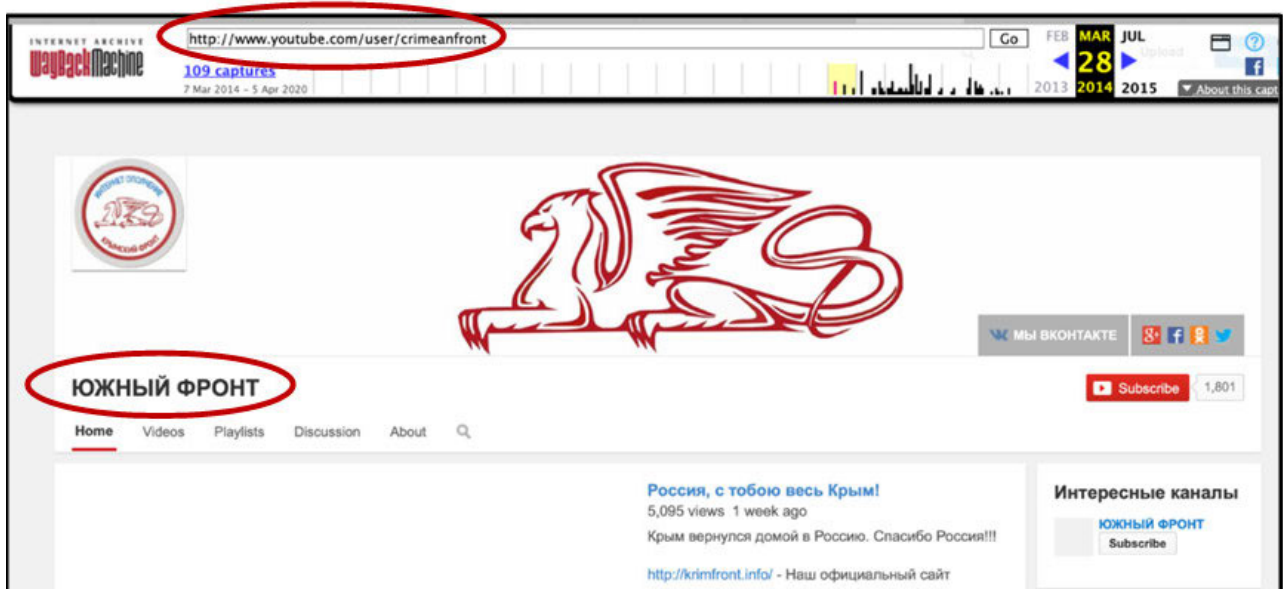


A screenshot of the archived VKontakte page.

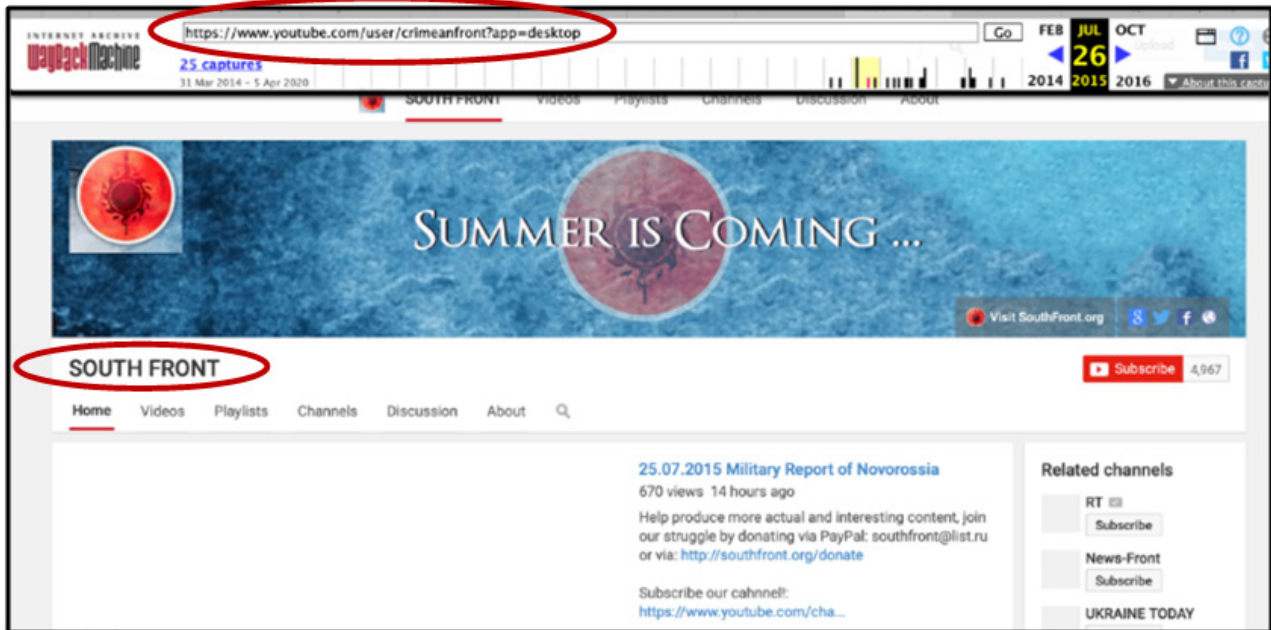
An examination of the archived pages of the *Crimean Front* YouTube account that *SouthFront* had claimed as its own demonstrates its transformation from Крымский Фронт (*Crimean Front*) to Южный Фронт (*Southern Front*) to *SouthFront*. The names of the page change but the YouTube URL remains the same. A screenshot of the channel's 'About' page from 2016 confirms this evolution, showing the full *SouthFront: Analysis and Intelligence* name alongside the *Crimean Front* URL and a description very similar to the 'About' page on *SouthFront's* current website.¹⁵⁷



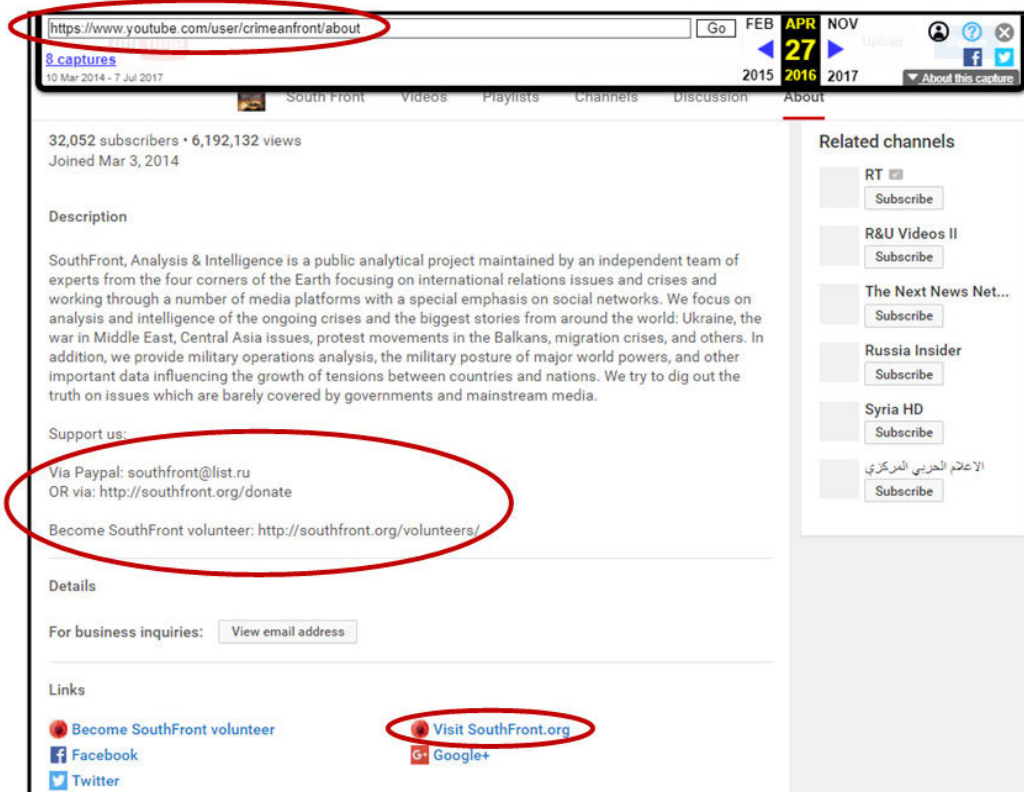
A screenshot of the archived YouTube page Крымский Фронт (Crimean Front).



A screenshot of the archived YouTube page Южный Фронт (Southern Front) showing via the circled URL that it is the same as the Крымский Фронт (Crimean Front) page.



A screenshot of the archived YouTube page South Front showing via the circled URL that it is the same as the previous Крымский Фронт (Crimean Front) and Южный Фронт (Southern Front) pages.



A screenshot of the channel's 'About' page showing the full SouthFront: Analysis and Intelligence name alongside the Crimean Front URL and a description very similar to the 'About' page on SouthFront's current website.

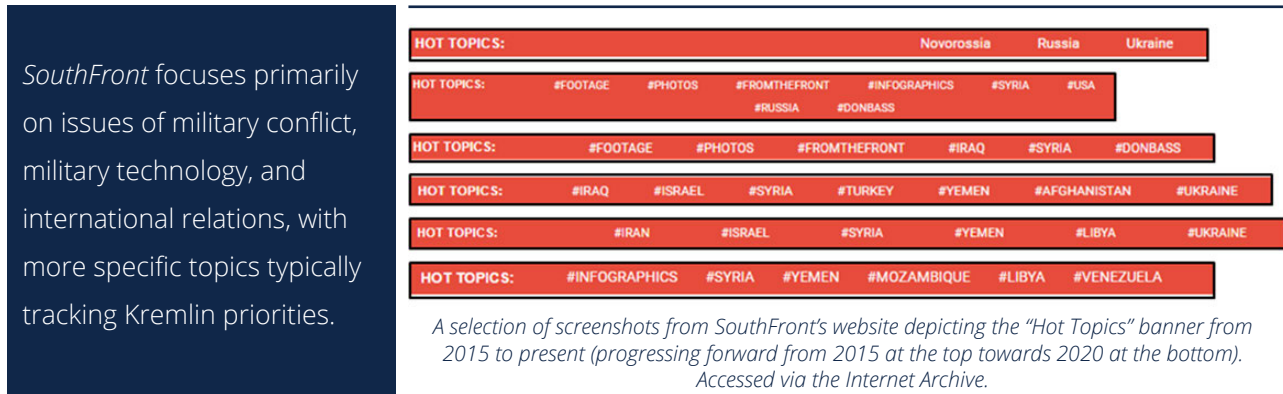
Denying Russian Links

Despite the evidence of its true origins and its Moscow registration, *SouthFront* goes to great lengths to appear not to be Russian. The website's [About page](#) says, "*SouthFront: Analysis & Intelligence* is a public analytical umbrella organization created and maintained by a team of experts and volunteers from the four corners of the Earth. ... Everybody can become a volunteer in our organization and share their own story and perspective with the world."¹⁵⁸ *SouthFront*'s PayPal address has a .ru address. The anonymous submission of content and reliance on [anonymous donations](#) provide additional layers of concealment to the site's managers.¹⁵⁹ There is no publicly-known owner or founder of *SouthFront*, though it has previously mentioned having a "Steering Committee."¹⁶⁰ Per a [denial](#) issued by *SouthFront* in reaction to a Bellingcat [report](#) on the outlet, "*SouthFront*'s founder is another person and all members of *SouthFront*'s Steering Committee know very well who he is."¹⁶¹

The metadata for at least the first 20 articles published by the outlet indicate that the same user account, uchfka32, is responsible for uploading all of these initial articles as well as many of the articles published recently. In addition to user account uchfka32, four other primary accounts appear to be the most prolific content uploaders in *SouthFront*'s metadata: JJs95, another_try, dim27348, and 9fjapsi_EE. It is difficult to attribute these user accounts to any of the *SouthFront* authors given that many articles are uploaded without authors or republished from other outlets. One possibility is that these user accounts belong to the members of the aforementioned "*SouthFront* Steering Committee," a group that is generally only mentioned in *SouthFront* [articles](#) pertaining to the 'censorship' of *SouthFront* social media properties or exposés on the outlet.¹⁶²

One person who openly claims to be on the Steering Committee is *SouthFront* Press Officer Viktor Stoilov, a Bulgarian [marketer](#) who runs a digital advertising and strategy [company](#) based in Sofia.¹⁶³ As of early June 2020, Stoilov had authored 82 articles for *SouthFront*, with his earliest article dating back to 16 June 2015. Other authors for *SouthFront* include J. Hawk, Daniel Deiss and Edwin Watson, who are often referred to as members of the "[SF Team](#)."¹⁶⁴ In addition to authoring articles on their own and in different group configurations, some of these authors also serve as translators. For example, J. Hawk is commonly credited as a translator from Russian to English for *SouthFront*.

Content



The below list is a sample of *SouthFront's* original content which directly aligns with Kremlin talking points and disinformation:

- ["Distraction Tactics: Reports of Chinese and Iranian Hacking, Russians Behind Protests"](#)¹⁶⁵
- ["How and Why the US Government Perpetrated the 2014 Coup in Ukraine"](#)¹⁶⁶
- ["Documentary on MH17 Reveals 5-Year-Long String of Lies"](#)¹⁶⁷
- ["Another Step Towards Ukraine-Like Scenario for Belarus"](#)¹⁶⁸
- ["The Venezuela-Iran Axis of Unity and Resistance Stands the Test of Time"](#)¹⁶⁹
- ["OPCW Manipulated Chemical Weapons Report On Syria's Douma by Removing Critical Details"](#)¹⁷⁰
- ["Russia Comments on U.S. Accusations Over Aleppo Chemical Attack, Says Washington is Trying to Whitewash Actions of Terrorists"](#)¹⁷¹

SouthFront also republishes [official Russian government statements](#), as well as content from official Russian state media outlets, such as [TASS](#) and [Sputnik](#).¹⁷² By distancing itself from Russia on paper, *SouthFront* aims to build a brand that provides "alternative viewpoints" while consistently pushing pro-Kremlin disinformation and propaganda. *SouthFront* has previously [responded](#) to [accusations](#) from EUvsDisinfo alleging it is a Russian disinformation outlet by citing isolated examples of when it has been critical of the Russian government—such as [criticizing](#) the Moscow government's "draconian" response to COVID-19—as proof that it is not serving Russian interests.¹⁷³ This tactic of dispensing a drop of seemingly honest water in an ocean of Kremlin-aligned disinformation is a common practice among outlets that aim to hide their links to Russia.

COVID-19 Disinformation

SouthFront's recent content includes disinformation and dangerous claims related to COVID-19. This includes posting articles authored by Peter Koenig of *Global Research*, an example of how sites in the ecosystem leverage each other's content. *SouthFront* [defends](#) Koenig's work as the product of an

individual with great professional experience, yet Koenig's writing is conspiracy-ridden and often rife with controversial rhetoric and [praise for authoritarian regimes](#).¹⁷⁴

The below examples of additional COVID-19 disinformation include both *SouthFront*-produced content and republication of disinformation from other outlets:

- ["Phenomena of Coronavirus Crisis:"](#) "Financial circles and governments are using the coronavirus to achieve own financial and political goals"¹⁷⁵
- [COVID-19 -- The Fight for a Cure: One Gigantic Western Pharma Rip-Off:](#) "The real question is – are vaccines – or a vaccine – even necessary? Maybe – maybe not. The production of vaccines is pushed for profit motives and for an important political agenda for a New World Order"¹⁷⁶
- [The Coronavirus COVID-19 Pandemic: The Real Danger is 'Agenda ID2020:'](#) "There is not the slightest trace of a pandemic... If indeed force-vaccination will happen, another bonanza for Big Pharma, people really don't know what type of cocktail will be put into the vaccine, maybe a slow killer, that acts-up only in a few years – or a disease that hits only the next generation – or a brain debilitating agent, or a gene that renders women infertile . all is possible – always with the aim of full population control and population reduction."¹⁷⁷
- [USA Plan: Militarized Control of Population. The 'National COVID-19 Testing Action Plan:'](#) "The 'pandemic response body' would above all have the task of controlling the population with military-like techniques, through digital tracking and identification systems, in work and study places, in residential areas, in public places and when travelling. Systems of this type – the Rockefeller Foundation recalls – are made by Apple, Google and Facebook."¹⁷⁸
- [Finally! EU Blames 'Kremlin Disinformation' for Coronavirus Crisis:](#) "EU bureaucrats and affiliated propaganda bodies are doing something that all has expected a long time ago – blaming Russia for the crisis over the outbreak of coronavirus."¹⁷⁹
- [COVID-19 Crisis in Russia: lockdown Craziness and Opposition Provocations:](#) "Summing up, it becomes obvious that anti-government Western-backed forces are trying to use the COVID-19 crisis to destabilize the situation in Russia."¹⁸⁰

Weak Lines of Defense

When *SouthFront* tries to [refute](#) claims it is proliferating Russian narratives, it generally falls back on two main arguments.¹⁸¹ The first is that *SouthFront* is an "international team of authors and experts" with no ties to any state. This fails to explain why *SouthFront* refuses to reveal its founder(s), Steering Committee

members, and main authors. The second line of defense is that *SouthFront* republishes articles from many other likeminded outlets often written by people with “advanced academic degrees.” Leveraging people with “advanced academic degrees” is a common tactic used by many outlets in the Russia’s disinformation and propaganda ecosystem, as detailed in this report.

Niche Graphics Capabilities

SouthFront also produces professionally designed [infographics](#), [maps](#), detailed “[Military Situation](#)” updates, and [videos](#) focused on troop movements, weapons systems, and conflict zones.¹⁸² These videos can now be found on *SouthFront*’s website under the header “SF TV” and on *SouthFront*’s [new YouTube channel](#), iterations of which have been removed by the platform in the past. Native English-speaking voiceover actors frequently narrate videos.¹⁸³



An example of one of SouthFront’s infographics depicting A Russian KH-35UE anti-ship missile



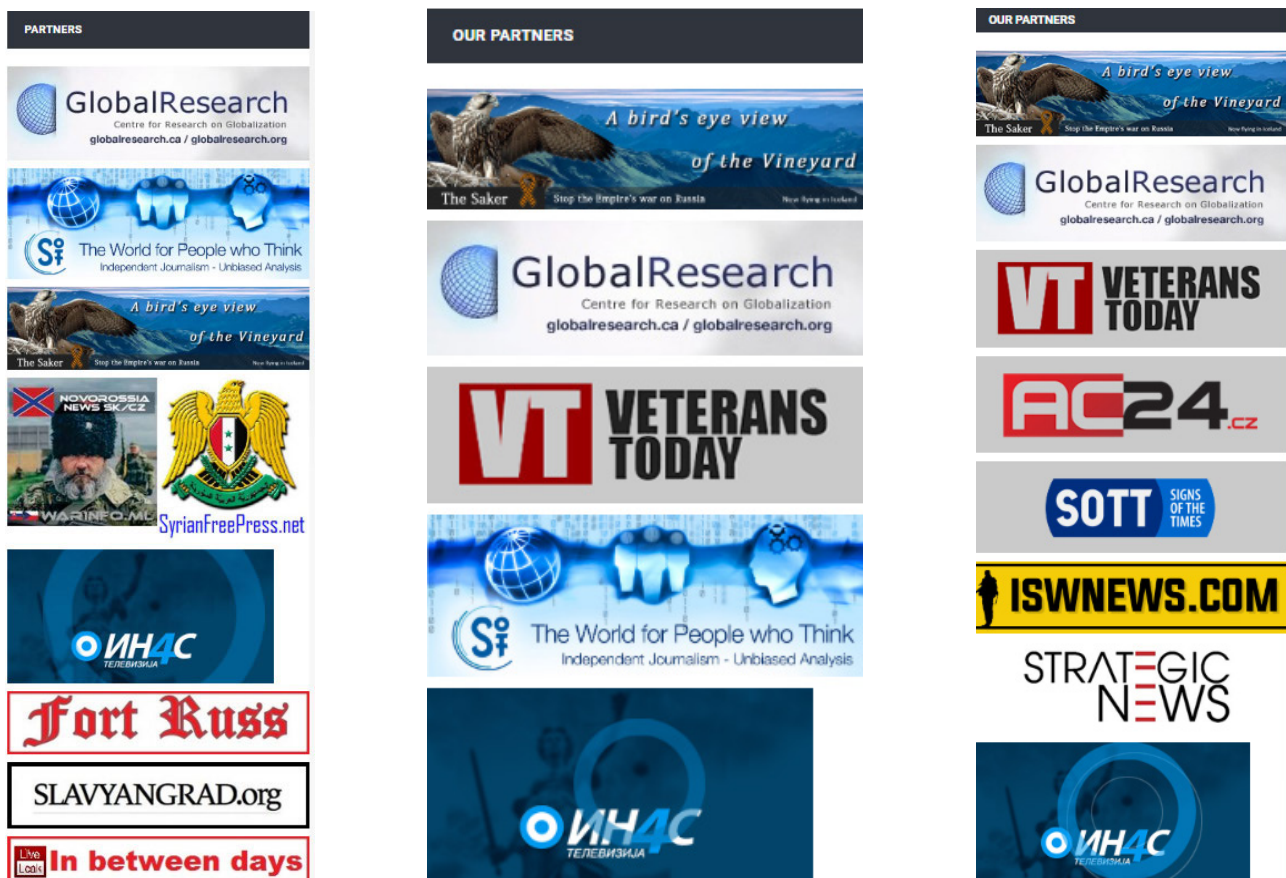
A SouthFront map depicting the military situation in Libya on June 10, 2020.



An example of one of SouthFront’s video “War Reports.”

Partners in the Ecosystem

From the beginning, *SouthFront* has officially partnered with other key players in the Russia's disinformation and propaganda ecosystem. As referenced in the profile on *Global Research*, *SouthFront* articles have been republished on *Global Research*'s website more than 1,200 times since mid-2015. As seen below, *SouthFront* once openly displayed its list of partners on its homepage and made frequent alterations to it. This changed sometime between 31 October 2018 and 6 November 2018 when the "Partners" column was removed from the website without explanation.

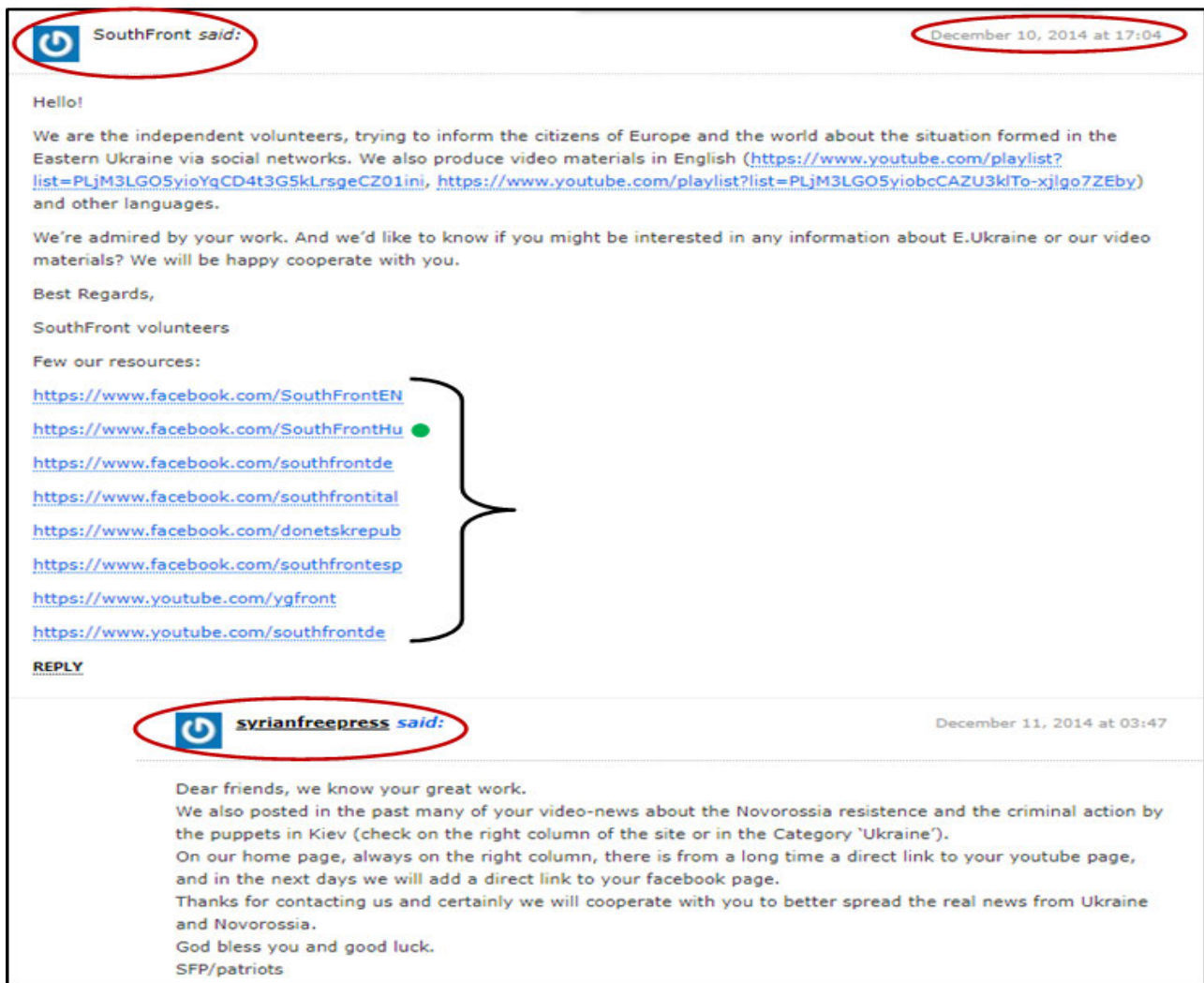


From left to right: SouthFront "Partners" columns from June 2015 to December 2015 and the last site screenshot of containing the "partners" column from 30 October 2018.

In addition to its stated partnership with *Global Research*, *SouthFront* has republished content from many other disinformation outlets, including the *Strategic Culture Foundation* and *New Eastern Outlook*. In many cases, this republication of content is mutual.

Syrian Free Press - A Window into Coordination

In an unusual instance of public coordination, *SouthFront* and one of its initial named partners, the *Syrian Free Press* site visible above, agreed on the latter's "[General-Contacts](#)" page to cooperate and "better spread the real news from Ukraine and Novorossia."¹⁸⁴ After this initial exchange from December 2014 (pictured below), the *SouthFront* user [follows up](#) on 24 April 2015 (immediately before the official registration of *SouthFront*) to ask that *Syrian Free Press* appeal to YouTube on its behalf to restore its original "SouthFront" channel and visit its new channel, "Crimean Front" (referenced earlier for its connections to *News Front*).¹⁸⁵ The *Syrian Free Press* editors [reply](#), saying "Job done. You will receive a private email from us."¹⁸⁶



A screenshot from Syrian Free Press' website showing an exchange between Syrian Free Press and SouthFront regarding potential cooperation.

SouthFront's Social Media Platforms as of June 2020

Platform	Language	Engagemen
Facebook	Hungarian	11,483 followers
	Multiple Accounts	Removed April 2020
Twitter	English	27,500 followers
	German	178 followers
YouTube	English English, multiple languages	Live - created 5 May 2020 - 7.08K subscribers Suspended 1 May 2020 (SouthFront requested that the Russian Foreign Ministry appeal on its behalf to no avail.) ¹⁸⁷

Proxy Site Profiles

Geopolitica.ru



Screenshot of a Geopolitica.ru article promoting conspiracy theories around Bill Gates.

Summary

Geopolitica.ru serves as a platform for Russian ultra-nationalists to spread disinformation and propaganda targeting Western and other audiences. Inspired by the Eurasianist ideology of the Russian philosopher and ultranationalist Alexander Dugin, *Geopolitica.ru* views itself as caught in a perpetual information war against the Western ideals of democracy and liberalism. The website's cooperation with other outlets in the Russia's disinformation and propaganda ecosystem broadens the reach of its messaging, which seeks to destabilize and weaken Western institutions. It publishes in English, Russian, Spanish, Italian, Serbian, French, Polish, Arabic, and Urdu.

Introduction - "Carthago Delenda Est"

[Geopolitica.ru](https://geopolitica.ru) is an online portal based in Russia which serves as a megaphone for the 'Eurasianist' ideas of the prominent ultranationalist Russian philosopher Alexander Dugin.¹⁸⁸ Dugin's [ideology](#) is based on the belief that "there is an irresolvable confrontation between the Atlanticist world (principally the United States and the United Kingdom) and Eurasia (predominantly Russia, Central and Eastern Europe

and Asia) that resists U.S.-led globalization and ethno-cultural universalization.”¹⁸⁹ This “resistance” is reflected in *Geopolitica.ru*'s slogan “Carthago delenda est” (Carthage must be destroyed), in which liberal democracies are [perceived](#) as the “Eternal Carthage” and Russia as the “Eternal Rome.”¹⁹⁰

Dugin gained notoriety for propagating [fascist views](#) and was reportedly influential in Kremlin circles, until [falling out of favor](#) for criticizing Russian President Vladimir Putin.¹⁹¹ According to Anton Shekhovstov, a scholar of Russian and European far right movements, Dugin was [dissatisfied](#) because Putin did not turn the 2014 attempted annexation of Crimea into a full conquest of Ukraine.¹⁹²

To realize its vision of weakening and eventually destroying the Western liberal world order that it posits as an enemy, *Geopolitica.ru* appears to follow the principles of the “program of subversion, destabilization, and disinformation” outlined by Dugin in his 1997 book *Foundations of Geopolitics*. He [advocates](#) using the Russian intelligence services “to introduce geopolitical disorder into internal American activity, encouraging all kinds of separatism and ethnic, social and racial conflicts, actively supporting all dissident movements—extremist, racist, and sectarian groups, thus destabilizing internal political processes in the U.S.”¹⁹³

Geopolitica.ru has connections with other sites and groups that also serve as proliferators of Russian disinformation and propaganda, especially [Katehon](#), as detailed below.¹⁹⁴

The “Eurasianist” Approach to a “Multipolar World”

[Established](#) in 2008 as a Russian-language website, *Geopolitica.ru* launched an [English-language page](#) in 2012, and between 2017 and 2019 [expanded](#) to include versions in Spanish, Italian, Serbian, French, Polish, Arabic, and Urdu.¹⁹⁵ The portal [describes](#) itself as “a platform for [the] monitoring of the geopolitical situation in the world” following the “Eurasian approach.”¹⁹⁶

Geopolitica.ru also claims to “promote a multipolar world,” while rejecting liberalism, communism, and fascism. The website’s proclaimed objection to fascism is disingenuous, considering Dugin’s reported [praise](#) for the projects of the Nazi paramilitary organization Schutzstaffel (SS) and its pseudo-research institute, the Ahnenerb.¹⁹⁷ The concept of the “multipolar world” championed by *Geopolitica.ru* translates into a [Dugin-envisioned world](#) where Russia dominates its neighbors: divides Georgia; annexes Ukraine, Finland, Serbia, Romania, Bulgaria and Greece; and “gives away” Azerbaijan to Iran.¹⁹⁸

In 2008, Dugin and his followers from the Eurasian Youth Union (a youth wing of Dugin’s Eurasia Party) [travelled](#) to the Russian-occupied Georgian region of South Ossetia.¹⁹⁹



Dugin and followers in South Ossetia in 2008

In 2015, Dugin was [sanctioned](#) by the United States along with other leaders of the Eurasian Youth Union for “actively [recruiting] individuals with military and combat experience to fight on behalf” of Russia-backed forces in Ukraine.²⁰⁰

Geopolitica.ru’s Role in Russia’s Disinformation and Propaganda Ecosystem

Some of the partners [listed](#) by *Geopolitica.ru* include the International Eurasian Movement (IEM), the [Center for Geopolitical Expertise](#), the [Center for Conservative Studies](#), and “some ex-members of the *Katehon* think tank,” all of which are affiliated with Dugin.²⁰¹ *Katehon*, where Dugin used to be a member of the supervisory board, is a pseudo-think tank with apparent links to the Russian state and intelligence services (see *Katehon* profile in this report). *Geopolitica.ru*’s [listed physical address](#) matched the same [address](#) occupied by *Katehon* until April 2019.²⁰² Its chief editor, [Leonid Savin](#), was formerly *Katehon*’s chief editor.²⁰³ Savin is affiliated with the IEM and is reportedly a member of the Military-Scientific Society of the Russian Ministry of Defense. Dugin is also an [associate](#) of *Katehon*’s sponsor, Konstantin Malofeyev.²⁰⁴ The United States [sanctioned](#) Malofeyev as “one of the main sources of financing for Russians promoting separatism in Crimea” and bankrolling “separatist activities in eastern Ukraine.”²⁰⁵

Geopolitica.ru and other proxy sites that proliferate Russian disinformation and propaganda often republish each other’s content. Savin, for example, is a regular contributor to the [Strategic Culture Foundation](#) (SCF).²⁰⁶ His articles are occasionally posted on [Global Research](#) and [Fort Russ News](#). He has also been featured on [NewsFront](#) and on the Russian state-funded media outlets [RT](#) and [Sputnik](#).²⁰⁷

Geopolitica.ru reprints articles from [Fort Russ News](#) including an [article](#) with disinformation that the [2016 ISIS terrorist attack](#) in Brussels was a false flag operation carried out by the United States and NATO.²⁰⁸ It also publishes content from [SCF](#), [Global Research](#), and the [New Eastern Outlook](#).²⁰⁹

Geopolitica.ru published 21 articles written by [Adomas Abromaitis](#),²¹⁰ a false persona [attributed](#) by Facebook to Russian Military Intelligence (GRU).

A sample of recent *Geopolitica.ru* articles on COVID-19 illustrates the false claims that it attempts to spread. They demonize the United States, promote anti-vaccine messaging, sow fear, and portray Europe as if it is in a state of collapse.

- [“Bill Gates vaccinations microchips and patent 060606”](#) promotes a conspiracy theory attacking Bill Gates and the Microsoft Corporation for an alleged plot to control humans by inserting microchips into their bodies. The article suggests a possible link between the Microsoft’s patent number WO/2020/060606 and the “number of the beast” from the “Book of Revelation.”²¹¹
- [“Russia and the coronavirus”](#) asserts that Western media spread disinformation about the number of COVID-19 related deaths in Russia and suggests that “one of the reasons why COVID-19 mortality rates are very low in Russia is that many Russians do not get flu vaccinations imported from the West.”²¹²
- [“New Malthusianism and the misanthrope dynasties”](#) falsely claims that the U.S. government and Bill Gates aim to reduce the world’s population, also alleging that Gates helped create the Zika virus.²¹³
- [“The Coronavirus and hybrid warfare”](#) speculates that COVID-19 is a part of a U.S. strategy “aimed at undermining the economic growth of both China and other countries” or a “plot by transnational capital against Donald Trump on the eve of the presidential election.”²¹⁴
- [“Former Putin’s aide: Coronavirus is the US biological weapon”](#) quotes Sergey Glazyev, a member of *Katehon’s* supervisory board member, an [associate of Dugin](#), and a former advisor to President Putin, as claiming that the COVID-19 virus is a U.S. biological weapon targeting “mostly people of the yellow race” and blaming Great Britain for provoking Hitler at the outbreak of World War II.²¹⁵
- [“Pandemic in the service of globalization”](#)– blames the EU/Atlanticist/Globalist powers for intentionally inflating the threat posed by the COVID-19 pandemic to “deepen the automation of society” for the benefit of “corporate capitalism” and the “world government.”²¹⁶
- [“The Italian government at the time of the coronavirus”](#) argues that the coronavirus crisis in Italy demonstrates that “the values of the Germany-dominated EU are not the values of the Italian people, and that the EU’s economic recipes have been lethal for Italy.”²¹⁷
- [“Pandemic and the survival policy: the horizons of a new form of dictatorship”](#) claims that COVID-19-related restrictive measures in Western societies amount to “total surveillance of the population” and will “gradually become permanent,” spelling the “end of liberal democracies and the establishments [sic] of dictatorships throughout the world.” This looming “dictatorship” is described as potentially “harsher than Nazi and Soviet concentration camps.”²¹⁸

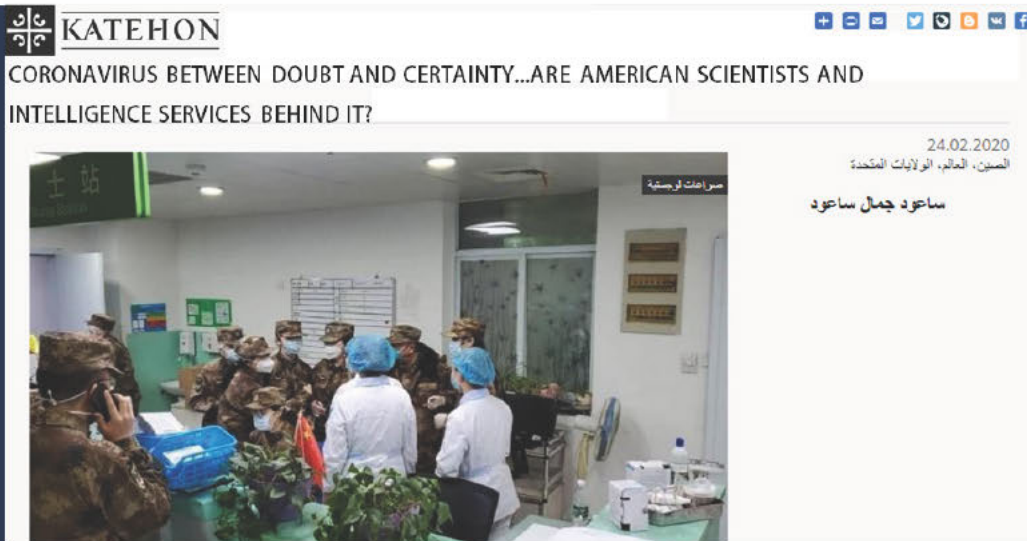
As [documented](#) by EUvsDisinfo, a project of the European External Action Service's East StratCom Task Force, additional disinformation narratives promoted by *Geopolitica.ru* included depicting the Western world as "[dominated by a handful of perverts](#)," alleging that [genocide](#) was committed against Russians in Ukraine, portraying [immigrants](#) in Europe as rapists, and trying to discredit [Western NGOs](#) by falsely accusing them of being CIA agents.²¹⁹

Geopolitica.ru's Social Media Platforms as of June 2020

Platform	Language	Engagement
Facebook	English	1,535 followers
	Russian	12,642 followers
	French	1,331 followers
	Spanish	1,557 followers
	Portuguese	32 followers, dormant since 2019
Instagram	Russian	55 followers
Twitter	French	247 followers, dormant since 2019
	Spanish	5000 followers
YouTube	Multilingual	2.86K subscribers 485,335 views
Vkontakte	Spanish	239 subscribers

Proxy Site Profiles

Katehon



Screenshot of a Katehon article translated from Arabic.

Summary

Behind the façade of a think-tank operation, Moscow-based *Katehon* is a proliferator of virulent anti-Western disinformation and propaganda via its [website](#), which is active in five languages. It is led by individuals with clear links to the Russian state. Within Russia's broader disinformation and propaganda ecosystem, *Katehon* plays the role of providing supposedly independent, analytical material aimed largely at European audiences, with content dedicated to "the creation and defense of a secure, democratic and just international system".

Introduction - Konstantin Malofeyev's Mouthpiece

Established in 2016, the Analytical Center *Katehon* is a [subsidiary](#) of *Tsargrad*, a company [founded](#) by Konstantin Malofeyev and affiliated with Malofeyev's pro-Kremlin *Tsargrad* TV, Russia's [self-described](#) "first conservative informational-analytical television channel" and the "voice of the Russian orthodox majority."²²⁰ The [website](#) publishes in five languages: English, Spanish, French, German, and Arabic.²²¹ The website also used to publish in Russian but has not done so since 2017.²²²

Often [referred](#) to as the "Orthodox oligarch," Malofeyev [runs](#) one of Russia's largest private foundations,

the St. Basil the Great Charitable Foundation.²²³ He is also the deputy head of the World Russia People's Council, an international organization led by the Russian Patriarch Kirill.²²⁴ Malofeyev is also the head of the "pro-Putin monarchist society" the Double-Headed Eagle; and [serves](#) on the Advisory Board of the Safe Internet League, a state-linked organization ostensibly [dedicated](#) to "fighting dangerous Web content" but [accused](#) by independent Russian media of "frequently blacklisting socio-political content."²²⁵ The [Chairman](#) of the Safe Internet League's Advisory Board is Malofeyev's [long-time associate](#) and Putin aide Igor Shchegolev. Shchegolev is the [Presidential Plenipotentiary Envoy to the Central Federal District](#) and a member of the [Security Council](#).²²⁶

According to independent Russian media outlet [The Bell](#), Malofeyev is currently "pursuing his ambition to lead a monarchist political party and build up a conservative media empire."²²⁷ In 2014, Malofeyev was sanctioned by the [United States](#) and the [European Union](#) for funding Russia-backed forces in Ukraine.²²⁸ In September 2019, Malofeyev established the International Agency for Sovereign Development (IASD), [described](#) by *Tsargrad TV* as the Russian attempt to "de-colonize" Africa and push the West out of the continent.²²⁹

State and Intelligence Ties

While claiming to be an independent organization, *Katehon's* leadership appears to have ties to both the Russian state and the Russian intelligence services. It is of note that the German, French and Arabic versions of *Katehon's* website do not mention the individuals serving on its [supervisory board](#), which in addition to Malofeyev include: ²³⁰

- Sergey Glazyev, President Vladimir Putin's [former economic advisor](#) and currently a Minister in charge of Integration and Macroeconomics at the [Eurasian Economic Commission](#).²³¹ Glazyev is under [U.S.](#) sanctions related to Russia's hostile actions in Ukraine.²³²
- Andrey Klimov, Deputy Chair of the Russian [Federation Council Committee on Foreign Affairs](#) and [Head](#) of the Council's Interim Committee for the Defense of State Sovereignty and the Prevention of Interference in the Internal Affairs of the Russian Federation.²³³
- Leonid Reshetnikov, a [retired](#) Lieutenant-General of the Russian Foreign Intelligence Service (SVR), where he led the Analysis and Information Department.²³⁴ Until 2017, Reshetnikov was the head of the [Russian Institute for Strategic Studies](#) (RISS), a Moscow-based think-tank that used to be a part of the SVR and now [conducts](#) research for the Kremlin.²³⁵ According to press reports, RISS research has included [plans](#) for Russian interference in the 2016 U.S. presidential elections and [proposals](#) for the Bulgarian Socialist Party to "plant fake news and promote exaggerated polling data" in advance of that country's presidential elections the same year.²³⁶ In 2016, RISS and *Katehon* co-authored a [report](#) allegedly analyzing U.S. ideology.²³⁷

- Alexander Makarov, a [retired](#) Lieutenant General of the Russian Federal Security Service (FSB).²³⁸

Since February 2017, *Katehon* has been [headed](#) by General Director Mikhail Yakushev, a Middle East scholar and the [Vice President](#) of the *St. Basil the Great Charitable Foundation*.²³⁹ Yakushev's career included stints at a [foundation](#) run by [Vladimir Yakunin](#), who is a U.S.-sanctioned Russian oligarch, former KGB officer, and former director of Russian Railways.²⁴⁰ Yakushev also held diplomatic posts in [Israel](#) and [Tunisia](#), and was [Chief of Staff](#) of the Russian Federation Council's Committee for Foreign Relations.²⁴¹

Additionally, in 2018, Yakushev [founded](#) the obscure *Center for International Strategic Initiatives*.²⁴² According to its English-language [website](#), which appears to be no longer operational but still accessible through the Internet Archive, the mission of the *Center for International Strategic Initiatives* is "to promote the realization of international initiatives in the interests of the public and private sector of Russia and developing Asia and Africa."²⁴³ The *Center* has received almost no coverage in Russian- and English-language press, but according to the a 2019 [article](#) in *Confidentiel Afrique*, its President Alexander Grachev, signed a memorandum of understanding with the President of the *Strategic Center of African Affairs*, Abdelmounem Boussafita, "for economic, social and political development between Russia and all African countries."²⁴⁴ Alexander Grigoriyevich Grachev is [listed](#) as one of the *Center's* leaders in the organization's registration documents and [appears](#) to have been Russia's former Consul General in Odessa, Ukraine and a Presidential Administration [official](#) responsible for interregional ties.²⁴⁵ In 2009, the *Kyiv Post* [reported](#) that the "Ukrainian government had allegedly demanded" Grachev's expulsion.²⁴⁶ According to the Ukrainian information agency *UNIAN*, Grachev was suspected of intelligence activities, including the recruitment of agents. *UNIAN* [cited](#) an article from the British Times claiming Grachev was financing pro-Russian groups in Ukraine.²⁴⁷

Conspiratorial Views of *Katehon's* Leadership

Katehon's leaders have promoted a variety of conspiracy theories:

- Glazyev, for example, [claimed](#) that COVID-19 was a U.S.-produced biological weapon; that Ukraine's President Volodymyr Zelensky (in cooperation with the United States and Israel) [planned](#) to ethnically cleanse the Russian-speaking population of eastern Ukraine and replace it with Israeli Jews; that the United States and its European partners have been [training](#) supposed Ukrainian neo-Nazis for the past 15 years; and that "[sinister forces of the 'new world order' conspired against Russia in the 1990s to bring about economic policies that amounted to 'genocide.'](#)"²⁴⁸
- Reshetnikov's eccentric worldviews [include](#) the conviction that the United States is determined to destroy Russia and masterminded World War II through its transnational companies.²⁴⁹ He also [argued](#) that the United States has created terrorist organizations and that its presidents have been selected by "secret powers."²⁵⁰

- Klimov, who has been [obsessed](#) with investigating “foreign agents,” sees a foreign hand in almost every domestic Russian affair that challenges the Kremlin’s line.²⁵¹ Recently, he accused U.S. diplomats, YouTube, and a Russian rapper who allegedly holds dual citizenship, of organizing protests against the Moscow Duma elections.²⁵² While purporting to be a champion of Russian sovereignty, Klimov headed a Cyprus-based company and ran a business with a British offshore company, according to a 2017 [article](#) from the independent Russian newspaper Novaya Gazeta.²⁵³

Disinformation and Conspiracy Theories Promoted on *Katehon’s* Website

Katehon is frequently cited as a source of disinformation in the [EUvsDisinfo database](#), a product of the European External Action Service’s East StratCom Task Force.²⁵⁴ It promotes false claims ranging from conspiracy theories attacking George Soros, the Rothschild family and the Pope, to disinformation and propaganda that seeks to undermine the EU, NATO, and trans-Atlantic solidarity. *Katehon’s* sites have also spread false allegations regarding COVID-19, including the below narratives catalogued in the EUvsDisinfo database:

- the British House of Commons considers the coronavirus a blessing;
- the coronavirus is a French-made virus transferred by the Americans;
- the coronavirus is an ethnic biological weapon;
- the coronavirus is a U.S. tool to disrupt Chinese production;
- the United States owns the coronavirus and its cure;
- the original source of the coronavirus is a U.S. military biological warfare laboratory;
- the United States created coronavirus in 2015; and
- science doubts the effectiveness of vaccines.

Katehon also promotes messages aimed at undermining European solidarity, claiming that supposedly traditional values are under attack, including:

- Europe is in danger because of Ukraine’s gas;
- Italy is being punished by the European Commission for supporting traditional values;
- the EU has Nazi roots; and
- Sweden’s feminist government orders not to investigate rapes to protect the immigrants that committed them.

Other disinformation that *Katehon* has promoted includes:

- Pope Francis is a servant of George Soros and the global Zionist conspiracy;
- George Soros’ tentacles entangle politics and generate chaos around the world;
- the Luciferian Zionist Rothchild crime family controls the Western mainstream media;

- the Holocaust was instigated by the evil Rothschilds for creating their own nation state;
- Rasputin was killed by the Anglo-Zionist empire; and
- the fire at the Notre Dame was a satanic ritual.

Katehon published 17 articles written by [Adomas Abromaitis](#), a false persona [attributed](#) by Facebook to Russian Military Intelligence (GRU).²⁵⁵

***Katehon* as a Tool in Pro-Kremlin Campaigns**

Katehon appears to have been established to advance the Kremlin's influence abroad with a specific focus on gaining audiences among fringe European elements. Its [website](#) features content in Russian, English, Spanish, French, German, and Arabic.²⁵⁶ When the website [first appeared online](#) in 2015, it also included Italian, Portuguese, Greek, Serbian, and Slovenian pages.²⁵⁷

According to media [reports](#), Malofeyev has served as a proxy for Kremlin priorities in Europe, sponsoring meetings and conferences of ultra conservative parties, as well as [directly](#) funding politicians and opinion makers who criticize liberal values and support the Kremlin's policies.²⁵⁸ Reportedly, Malofeyev was involved in the purported annexation of Crimea, support for the Russian military-backed [separatist militancy in Donbass](#), election meddling in [Bosnia and Herzegovina](#), and media acquisition in Greece, Bulgaria, and Serbia. *Katehon* promotes these same overarching goals through its disinformation and propaganda activities.²⁵⁹

Additionally, *Bellingcat* [found](#) "circumstantial evidence" that Malofeyev was involved in the failed 2016 coup in Montenegro aimed to [prevent](#) that country from joining NATO.²⁶⁰ Montenegrin officials [claimed](#) that *Katehon* board member Leonid Reshetnikov also played a key role in the organization of the coup.²⁶¹ In 2019, Bulgaria [banned Malofeyev](#) and [Reshetnikov](#) from entering the country for ten years in connection with espionage and money laundering charges against Nikolai Malinov, chairman of the pro-Kremlin Bulgarian National Movement of Russophiles and a recipient of the Order of Friendship award from President Putin.²⁶²

A prominent Russian philosopher, ultranationalist, and the leader of the [International Eurasian Movement](#), Alexander Dugin (see *Geopolitica.ru* case study) was a *Katehon* [board member](#) and the [chief editor](#) of *Tsargrad TV* until 2017.²⁶³ Dugin has reportedly been one of the key [drivers](#) behind Malofeyev's strategy to establish a network of pro-Kremlin politicians among the ranks of [European radicals](#).²⁶⁴ The U.S. Department of Treasury [sanctioned](#) Dugin for "being responsible for or complicit in actions or policies that threaten the peace, security, stability, or sovereignty or territorial integrity of Ukraine."²⁶⁵

In 2014, a Russian hacking group [Shaltay Boltay](#) (also known as *Anonymous International*) published email correspondence of [Georgi Gavrish](#), an associate of Dugin and former officer at the Russian embassy in Athens.²⁶⁶ The released materials included a [memorandum](#), allegedly penned by Dugin, mapping out the European far-right into three broad factions: the Christian right, the Neo-Nazis, and the New Right.²⁶⁷ Dugin predicted that these actors would become “an essential factor in Russian-European relations,” arguing that the “extremely influential” New Right faction—consisting of parties like the French National Front, the Austrian Freedom Party, the Italian Northern League, and the Alternative for Germany—would be the most suitable partner for Russia, as it “has a sympathy for Orthodoxy, supports Russia and Putin, consistently stands on anti-American and anti Atlantist positions.” Dugin also [claimed](#) that the CIA and the Mossad control the neo-Nazi movements in Europe, which are often led by Jews and homosexuals.²⁶⁸

Another insightful [item](#) from Gavrish’s correspondence was a document containing a [list](#) of foreign contacts with whom Dugin supposedly discussed creating a pro-Russian “information initiative.”²⁶⁹ The list was composed largely of European but also South American, Middle Eastern, and Asian politicians and journalists. [Christo Grozev](#) and [Anton Shekovstsov](#) have suggested that Dugin’s analysis led to the creation of *Katehon*, which began operating shortly after the memorandum was written, and features “many authors” from the foreign contacts list.²⁷⁰

Katehon’s Social Media Platforms as of June 2020

Platform	Language	Engagement
Facebook	English	12,155 followers
	Spanish	page currently unavailable
	Arabic	49,863 followers
	French	page currently unavailable
	German	page currently unavailable
	Russian	775 followers, not updated since 2016
Instagram	Katehon news	70 followers
Twitter	English	Account suspended
	Spanish	Account suspended
	French	Account suspended
	Arabic	357 followers
	German	33 followers, no new posts since 2017
	Russian	828 followers, no new posts since 2016
YouTube	English	5.93K subscribers, 1,069,466 views, most recent video uploaded 2 years ago
	Serbian	24 subscribers, most recent video uploaded 4 years ago

Digital Media Analysis

Summary:

Between February and April 2020, the seven Kremlin-aligned disinformation proxy sites and organizations profiled in this report amplified narratives critical of the United States and favorable to Russian positions, particularly in relation to the COVID-19 outbreak.

Four of the outlets—*Global Research*, *SouthFront*, *New Eastern Outlook*, and *Strategic Culture Foundation*—were observed publishing one another's content on 141 occasions, indicative of possible collaboration among them. Published content appeared in a variety of languages and was shared across multiple social media platforms.

Website Analytics

The Global Engagement Center (GEC) analyzed web traffic to seven Kremlin-aligned proxy sites and organizations and their sub-domains between 1 February and 30 April 2020.²⁷¹ The table below displays the number of page visits, the number of articles published, and the average potential readership per article for each outlet during this period. As the table shows, *Global Research*, *News Front* and *SouthFront* received the most page visits and published the most articles over the three months; however, there were vast differences in the potential sizes of their readerships.²⁷²

At more than 350,000 potential readers per article, no other outlet had half as much reach as *Global Research*; in fact, despite authoring the greatest number of articles, *News Front* had only 12% of the number of potential readers per article (nearly 42,000), the third lowest overall. By contrast, *Geopolitica.ru* authored the second fewest articles but had the second highest potential readership per article; at more than 145,000, it was 41% the size of *Global Research's* potential readership.

Site	Number of Page Visits ^A	Number of Articles Published	Average Potential Readership per Article ^B	Ratio of Potential Readers/Article vs. Global Research ^C
Global Research	12,370,000	2,307	351,247	--
News Front	8,950,000	3,617	41,895	0.12
SouthFront	4,300,000	1,546	126,411	0.36
Geopolitica.ru	1,480,000	224	145,304	0.41
Strategic Culture Foundation	990,000	420	48,789	0.14
New Eastern Outlook	540,000	402	17,667	0.05
Katehon	225,000	26	17,982	0.05

^A Page visits data was retrieved from SimilarWeb on 1 July 2020 and includes outlets' main websites and sub-domains, where available.

^B SimilarWeb potential readership is defined as the number of people who potentially saw an article based on the number of unique visitors to the publication's website.

^C Values in this column represent the relative rate of potential readership, controlling for number of articles published, compared to Global Research, which had 351,247 potential readers per article published between 1 February and 30 April 2020.

Amplification of Russian Narratives

During the period of analysis, the seven outlets consistently embraced positions reflective of the Russian government and state-funded media. They [reposted](#) or [referenced](#) RT content (92 mentions), [reposted](#) or [referenced](#) Sputnik content (78 mentions), and [referenced](#) Russian MFA Spokesperson Mariya Zakharova (35 times).²⁷³ These articles included opinion pieces, long-reads, and short articles, including some with links to videos.

Senior Russian officials and pro-Russian media sought to capitalize on the fear and confusion surrounding the COVID-19 pandemic by actively promulgating conspiracy theories. For example, they promoted conspiracy theories centered around false U.S. bioweapon infrastructure. We observed five of the seven outlets promoting this narrative across 30 articles. On 20 February, *New Eastern Outlook* published an article in both [Russian](#) and [English](#) claiming that the U.S. deployed a biological weapon against China.²⁷⁴



Screenshot from a New Eastern Outlook article.

Then on 22 February, *News Front's* Bulgarian language edition [published](#) an adapted version of the same article.²⁷⁵ On 5 March, *RT* [published](#) an article, titled "Coronavirus May Be a Product of US Biological Attack Aimed at Iran and China, IRGC chief claims" which was [re-published](#) by *Global Research* on 6 March and then by *News Front's German* edition on 9 March.²⁷⁶ On 16 March, the narrative evolved to suggest the U.S. military had [used](#) a bioweapon in Cuba, and on 18 March, another *Global Research* [article](#) asserted that China considers the virus to be a bioweapon.²⁷⁷ On 20 March, *News Front* [insinuated](#) that a U.S. lab in Georgia was involved in the creation of the coronavirus—a narrative *News Front* continued to promote throughout the period examined.²⁷⁸

Cross-Platform Content Amplification

Among the seven media outlets, four were observed frequently re-posting one another's content. Specifically, among *Global Research*, *New Eastern Outlook*, *SouthFront*, and *Strategic Culture Foundation*, 141 articles were originally posted by one outlet and later re-posted by another during the three-month period of analysis. Of particular note, *Global Research* re-posted 50 [videos](#) originally published by *SouthFront*.²⁷⁹ Because of this pattern of cross-posting content, these four outlets formed an especially interconnected set of nodes within the broader network of the seven websites examined. Below is a sample of articles that were recycled from one outlet to another, which demonstrates the variety of sources that potentially collaborated, the range of topics that were covered, and the varying durations between original and republication dates:



These four outlets often re-published their own articles in more than one language. *Global Research* posted in [Italian](#), [French](#), and [English](#),²⁸⁰ *New Eastern Outlook* in [English](#) and [Russian](#),²⁸¹ *News Front* in [Bulgarian](#) and [German](#),²⁸² and *SouthFront* in [English](#) and [German](#).²⁸³ Although these outlets tended to post one another's content, they did not tend to post translated versions of another site's content; article translations were only observed within each site.

Content Engagement by Shares on Social Media

Among the 8,542 articles published by the seven outlets between 1 February and 30 April, 1,941 (23%) were shared on Twitter via 20,670 tweets. A *Global Research* [article](#) titled "China's Coronavirus: A Shocking Update. Did the Virus Originate in the US?" posted on 4 March was among the top-five most shared articles in the data set (424 tweets). The article has since been removed by *Global Research*, but it is still referenced on the social media platform Reddit and by fringe media sites.²⁸⁴ A *News Front* Spanish edition [article](#) titled "Hell in New York: One Coronavirus Death Every 17 minutes: Doctors Can't Keep Up" was shared via 388 tweets, propelling a narrative aimed at undermining public trust in the U.S. national healthcare system.²⁸⁵ The most-shared Russian-language [article](#) (shared via 221 tweets) was published by *News Front*, and speculated that the EU budget under negotiation would substantially decrease support to the Baltic countries.²⁸⁶



Screenshot from a *News Front* Serbia article containing the message "From Russia with Love" to underscore Russia's COVID-19 assistance to Serbia.

In addition to Twitter, 137 articles (1.6%) were shared 15,052 times on Facebook. A *News Front* Bulgaria article praising Russia's assistance to Serbia during the coronavirus pandemic received the greatest number of Facebook shares—a total of 2,000.²⁸⁷ The second-most shared [article](#) (1,381 shares) was published by *News Front Bulgaria* and reported that, according to a survey published in *Foreign Affairs*, residents of Crimea were confident that Russia would withstand the pressure of sanctions imposed by the United States and other Western countries.²⁸⁸ The third-most shared [article](#) on Facebook was published by *SouthFront*, and reported on the killing of a senior al-Qa'ida commander in a Russian airstrike on 12 February in Western Aleppo.²⁸⁹

Twitter Analysis

Summary

The GEC analyzed Twitter mentions of seven Kremlin-aligned proxy sites and organizations: *Global Research*, *News Front*, *SouthFront*, *Strategic Culture Foundation*, *Geopolitica.ru*, *Katehon* and *New Eastern Outlook*. Twitter mentions included tweets and re-tweets that linked to articles published by these outlets, either from the outlets' Twitter accounts or from other users linking to the articles. Of these seven outlets, *Global Research* and *SouthFront* have the largest presence on Twitter, as judged by the number of Twitter accounts they operate and the number of followers on each account. However, in terms of Twitter mentions, all seven outlets had their articles disseminated on the platform. Accounts tweeting these articles during the reporting period were geotagged to the UK (16%), Russia (9%), and Canada (7%). The most popular hashtags #covid19 and #coronavirus—along with a manual analysis of most-shared content, suggest that COVID-19 was the primary focus.

Outlet	Mentions
Global Research	85,055
News Front	29,955
SouthFront	26,822
Strategic Culture Foundation	17,213
Geopolitica.ru	6,989
New Eastern Outlook	5,116
Katehon	2,099

Report

From 1 April through 30 June 2020, the GEC identified 173,000 tweets and retweets that included links to these outlets. The table displays the number of times each outlet was linked to (mentioned) on Twitter.

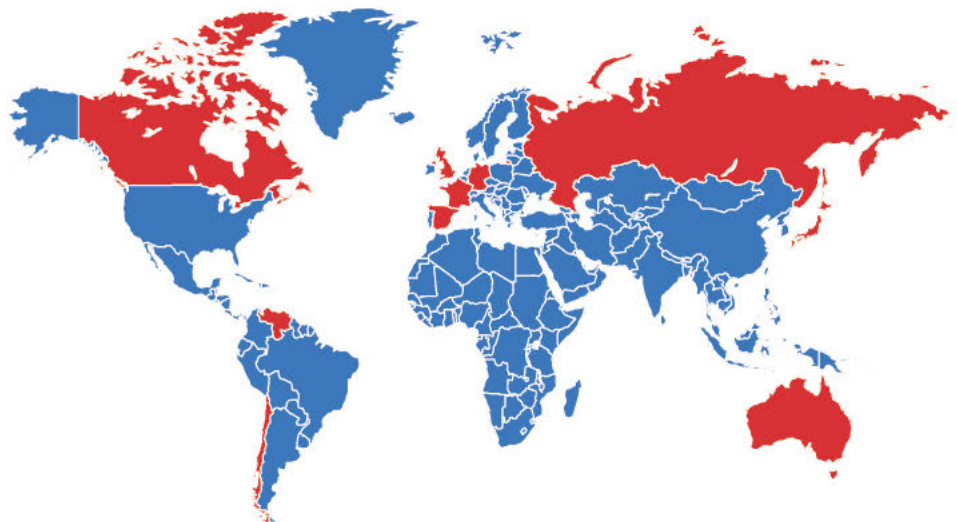
Except for *Global Research* and *SouthFront*, the examined outlets have a relatively limited Twitter presence—*News Front*'s Twitter accounts have all been suspended and *New Eastern Outlook* does not have an active Twitter account. Nevertheless, content from these outlets is still shared widely on the platform. Approximately 59,000 accounts globally, excluding those in the United States, shared articles from these outlets during the reporting period. However, most of this activity came from a concentrated group of active accounts. About 1% of all the accounts in the query tweeted more than 35% of tweets sharing these articles, while the top 0.1% of accounts tweeted almost 18% of the tweets in our sample.

Account	Outlet	Followers	Last Active
@CRG_CRM	Global Research	37.4K	Present
@southfronteng	SouthFront	27.8K	Present
@GRTVnews	Global Research	19.8K	Nov 2018
@Strateg_Culture	Strategic Culture Foundation	5.6K	May 2020
@Geopoliticaesp	Geopolitica.ru	5.0K	Present
@geopolitica_FR	Geopolitica.ru	262	May 2019
@KatehonA	Katehon	368	Present

Of the 0.1% most active accounts, *News Front* was the sole outlet never tweeted by accounts tweeting articles from multiple outlets. *Global Research* and *New Eastern Outlook* were the two outlets that were most likely to be tweeted by the same account. Several of the most active accounts shared content from more than half of the outlets included in our analysis, where articles frequently spread sensationalized or questionable content, including outright disinformation. For more information regarding cross-platform content amplification among these outlets, please see the Digital Media Analysis section of this report.

According to self-reported locations, accounts tweeting these articles were concentrated in the following top ten locations:

1. UK (16%)
2. Russia (9%)
3. Canada (7%)
4. Japan (6%)
5. France (5%)
6. Spain (4%)
7. Chile (4%)
8. Venezuela (4%)
9. Germany (3%)
10. Australia (3%)

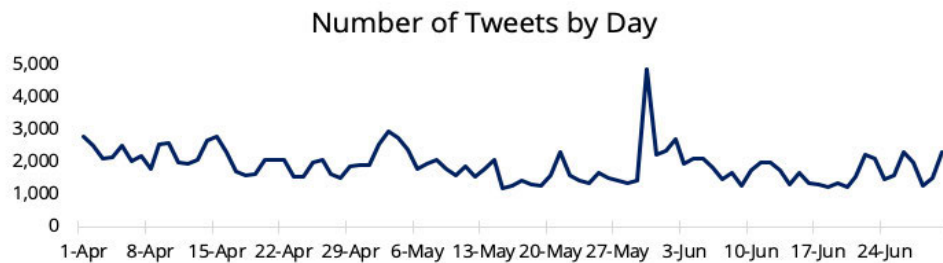


Given its prominence in the dataset, many of the overarching topics reflected the narratives promoted by *Global Research*. Across the entire dataset of tweets that amplified articles from the outlets included in this report, the most used hashtags were:

1. #covid19 (4,358 tweets)
2. #coronavirus (2,265 tweets)
3. #us (949 tweets)
4. #billgates (867 tweets)
5. #china (718 tweets)

The daily tweet volume was relatively stable across the period examined, except for a dramatic peak on 30 May. This peak was driven by extensive sharing of a *Strategic Culture Foundation* [article](#) claiming that a German official leaked a report denouncing COVID-19 as “A Global False Alarm.”²⁹⁰ This article, which contains misinformation downplaying the threat of COVID-19, was the most shared article—tweeted more than 15,000 times—during the reporting period. The report at the center of the article was [denounced](#) by the German government as the work of a lone employee who used the German Federal Ministry of the Interior (BMI)’s official letterhead to support the employee’s private opinion.²⁹¹ The *Strategic Culture Foundation* article also references an *RT* [article](#) that includes a press release defending the BMI employee

and criticizing the German Federal Ministry.²⁹² Although the central claims of the report have been refuted—the report was [fact-checked](#) by Health Feedback as “unsupported” and [criticized](#) by Der Spiegel for exaggerating and citing “dubious blogs”—*Strategic Culture Foundation* endorsed the false claims.²⁹³



While the most widely shared article originated from the *Strategic Culture Foundation*, *Global Research* was the most prominent outlet, accounting for almost half of all the articles shared on Twitter. Most of *Global Research*'s content included sensationalized coverage or disinformation about COVID-19 and vaccines, often featuring false claims about the U.S. government or Bill Gates. Although COVID-19 disinformation was the most prominent topic, conspiracy theories were mixed in, many of them making accusations against the United States or U.S. citizens. The most widely shared articles included:

- [“‘Greater Israel’: The Zionist Plan for the Middle East”](#) (2,656 tweets);²⁹⁴
- [“US Hospitals Getting Paid More to Label Cause of Death as ‘Coronavirus’”](#) (2,427 tweets);²⁹⁵ and
- [“‘Mass Sterilization:’ Kenyan Doctors Find Anti-fertility Agent in UN Tetanus Vaccine”](#) (2,127 tweets).²⁹⁶

News Front was the second-most shared outlet on Twitter during the reporting period. Popular content from this outlet focused on pro-Russian narratives and geopolitics related to the United States, Eastern Europe, and Latin America. Its most popular content was written in Russian and Spanish. The most widely shared articles included:

- [“Alexander Rogers: Those who betrayed their homeland lose their talent”](#) (1,223 tweets);²⁹⁷
- [“Swedish-Palestinian journalist dies just before exposing Soros and Aschberg”](#) (873 tweets);²⁹⁸ and
- [“Supreme Court of Brazil asks to suspend Bolsonaro for 180 days due to its inefficiency against the coronavirus”](#) (434 tweets).²⁹⁹

The most popular articles from *SouthFront*, the third-most shared outlet in this analysis, focused on conspiracy theories related to COVID-19, conflict in the Middle East, and criticism of the United States. Accounts sharing content from this outlet were concentrated in Japan and European nations. Most of the Japanese activity was from accounts associated with “QAnon,” a conspiracy theory focused on the “deep state.” The most widely shared articles included:

- [“THE CORONAVIRUS COVID-19 PANDEMIC: THE REAL DANGER IS ‘AGENDA ID2020’”](#) (881 tweets);³⁰⁰
- [“SOUTHFRONT’S YOUTUBE CHANNEL IS BANNED”](#) (760 tweets);³⁰¹ and
- [“U.S. USED \\$601M SEIZED FROM VENEZUELA TO FUND BORDER WALL WITH MEXICO”](#) (665 tweets).³⁰²

Strategic Culture Foundation was the fourth-most shared outlet in our analysis, with the majority of tweets linking to the article mentioned above. Other popular content from the outlet also focused on COVID-19-related disinformation that made references to the U.S. government and Bill Gates. The most widely shared articles included:

- [“German Official Leaks Report Denouncing Corona as ‘A Global False Alarm’”](#) (15,020 tweets);³⁰³
- [“Is It Time to Launch an Investigation Into the Bill & Melinda Gates Foundation for Possible ‘Crimes Against Humanity?’”](#) (418 tweets);³⁰⁴ and
- [“What Did U.S. Intel Really Know About the ‘Chinese’ Virus?”](#) (302 tweets).³⁰⁵

Geopolitica.ru, the fifth-most shared outlet, was most popular among accounts in Spanish-speaking countries including Chile, Spain, and Venezuela. Popular content from the outlet highlighted criticism of the United States, George Soros, and the modern day Western anti-fascism movement. The most widely shared articles included:

- [“PUTIN: 95% OF WORLD TERRORIST ATTACKS ARE MADE BY THE CIA”](#) (1,963 tweets);³⁰⁶
- [“SOCIAL ENGINEERING: GLOBALIST SOROS WANTS ABORTIONS WORLDWIDE”](#) (676 tweets);³⁰⁷ and
- [“ANTI \(FASCISTS\): THE GLOBALISTS’ ARMY OF TERROR”](#) (1,963 tweets).³⁰⁸

New Eastern Outlook, the sixth-most shared outlet, focused on English-language articles related to COVID-19. These articles criticized the United States and “big pharma.” The most widely shared articles included:

- [“Why is Trump Drumbeating a ‘New Cold War’ with China?”](#) (1,078 tweets);³⁰⁹
- [“The Remarkable Doctor A. Fauci”](#) (286 tweets);³¹⁰

Katehon was the least-shared outlet on Twitter in our analysis. Most of the accounts sharing this content were located in Europe. Many of the popular topics focused on criticizing and exposing the global “deep state.” The most widely shared articles included:

- [“WHO IS ENRICO SASSOON GODFATHER OF “CASALEGGIO ASSOCIATI” AND “5 STAR MOVEMENT”?”](#) [\(454 tweets\)](#),³¹¹
- [“THE HUB OF WORLD EVIL: THE BRITISH DEEP STATE”](#) (182 tweets);³¹² and
- [“EUROPE: ON THE EVE OF THE CIVIL WAR?”](#) (43 tweets).³¹³

References

- ¹ <https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>
- ² <https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.html>
- ³ <https://www.rusprofile.ru/id/4627728>
- ⁴ <https://web.archive.org/web/20100908070545/http://www.strategic-culture.org/>
- ⁵ <https://www.nytimes.com/2020/07/28/us/politics/russia-disinformation-coronavirus.htmlhttps://www.strategic-culture.org/>
- ⁶ <https://www.strategic-culture.org/>
- ⁷ <http://en.interaffairs.ru/>,
- <http://en.interaffairs.ru/partners.html>
- ⁸ <https://www.rusprofile.ru/id/4627728>,
- <https://www.latimes.com/archives/la-xpm-1989-11-22-mn-152-story.html>,
- <https://www.washingtonpost.com/archive/politics/1990/07/15/soviets-weaken-party-politburo/e704c942-2e22-4157-8236-6c36e636897d/>
- ⁹ <https://www.rusprofile.ru/founders/3857002>
- ¹⁰ <https://xn--n1aaccga-xn--p1ai/>
- ¹¹ <http://www.edinaya-odessa.org/st/8850-russkoe-edinstvo.html>
- ¹² <https://web.archive.org/web/20150502152336/http://www.strategic-culture.org/>
- ¹³ <https://www.strategic-culture.org/>
- ¹⁴ <https://www.strategic-culture.org/contributors/?letter=C>
- ¹⁵ <https://www.strategic-culture.org/news/2013/03/10/us-psychotic-superpower-on-a-hair-trigger/>
- ¹⁶ <https://www.strategic-culture.org/news/2013/04/20/give-north-korea-some-respect/>
- ¹⁷ <https://www.strategic-culture.org/news/2014/04/18/putin-stands-out-as-a-real-world-leader/>
- ¹⁸ <https://www.strategic-culture.org/news/2015/04/26/washington-choreographing-all-out-war-with-russia/>
- ¹⁹ <https://www.strategic-culture.org/news/2015/01/03/the-year-us-led-capitalism-became-exposed-as-root-of-global-conflict/>
- ²⁰ <https://www.rt.com/op-ed/authors/Finian-Cunningham/>,
- <https://sputniknews.com/search/?query=finian+cunningham>,
- <https://ria.ru/search/?query=%D1%84%D0%B8%D0%BD%D0%BD%D0%B8%D0%B0%D0%BD+%D0%BA%D0%B0%D0%BD%D0%BD%D0%B8%D0%BD%D0%B3%D0%B5%D0%BC>
- ²¹ <https://www.strategic-culture.org/contributors/?letter=C>
- ²² <https://www.strategic-culture.org/news/2020/04/14/the-facts-about-crimea-should-be-recognised-and-so-should-crimea/>,
- <https://www.strategic-culture.org/news/2019/11/19/washington-wants-an-arctic-circle-of-confrontation/>
- ²³ <https://www.strategic-culture.org/contributors/?letter=E>
- ²⁴ <https://risingtidefoundation.net/about-us/>
- ²⁵ <https://orientalreview.org/2019/07/16/freeland-responds-to-putin-liberalism-will-prevail-nazis-will-help/>,
- <https://www.geopolitica.ru/en/article/londons-five-eyes-freelands-nazi-roots-stand-exposed-once-more>
- ²⁶ <http://canadianpatriot.org/about-us/>
- ²⁷ <https://risingtidefoundation.net/about-us/>,
- <https://www.strategic-culture.org/contributors/?letter=C>,
- <https://www.strategic-culture.org/news/2020/03/14/a-70-year-war-on-propaganda-built-by-the-cia/>
- ²⁸ <https://www.strategic-culture.org/contributors/?letter=K>,
- <https://www.voltairenet.org/auteur125978.html?lang=en>,
- <https://www.voltairenet.org/article187508.html>
- ²⁹ <https://www.strategic-culture.org/contributors/?letter=I>
- ³⁰ <https://www.strategic-culture.org/news/2015/05/01/modern-nazism-driving-force-euro-atlantic-integration/>
- ³¹ <https://www.strategic-culture.org/news/2015/02/13/the-czech-republic-doomed-without-russia/>
- ³² <https://www.strategic-culture.org/news/2014/10/05/estonia-doomed-without-russia/>
- ³³ <https://www.strategic-culture.org/news/2015/07/04/russia-has-enough-gas-for-everyone/>
- ³⁴ <https://www.strategic-culture.org/news/2015/07/21/brussels-kiev-duo-blackmailers/>
- ³⁵ <https://web.archive.org/web/20100908070545/http://www.strategic-culture.org/>,
- <https://web.archive.org/web/20110805041427/http://www.strategic-culture.org/>
- ³⁶ <https://journal-neo.org/about/>
- ³⁷ <https://www.ivran.ru/en/periodicals>
- ³⁸ <https://journal-neo.org/>
- ³⁹ <https://journal-neo.org/author/christopher-black/>
- ⁴⁰ <https://journal-neo.org/2014/12/29/cuban-resistance-an-example-for-the-world/>
- ⁴¹ <https://journal-neo.org/2015/01/22/paris-and-volnovakha-the-brutal-face-of-nato-terrorism/>
- ⁴² <https://journal-neo.org/2017/04/17/america-aggression-a-threat-to-the-world/>
- ⁴³ <https://journal-neo.org/2018/03/09/the-skripal-incident-another-anti-russian-provocation/>
- ⁴⁴ <https://journal-neo.org/2019/03/15/war-against-venezuela-is-war-against-us-all/>
- ⁴⁵ <https://journal-neo.org/author/peterkoenig/>
- ⁴⁶ <https://journal-neo.org/2020/02/28/china-confronts-covid19-with-endless-creation-towards-a-shared-future-for-mankind/>
- ⁴⁷ <https://journal-neo.org/author/james-oneill/>
- ⁴⁸ <https://ahtribune.com/>,
- <https://www.cnn.com/2020/01/24/tech/iran-info-ops/index.html>
- ⁴⁹ <https://www.strategic-culture.org/>
- ⁵⁰ <https://www.nationalreview.com/2003/04/still-red-ion-mihai-pacepa/>,
- <https://www.latimes.com/archives/la-xpm-1990-01-28-mn-1248-story.html>
- ⁵¹ <https://www.nationalreview.com/2003/04/still-red-ion-mihai-pacepa/>
- ⁵² <https://www.workers.org/2019/10/43954/>,
- <https://www.workers.org/2020/04/47443/>,
- <https://www.workers.org/2019/01/40259/>
- <https://www.workers.org/2018/02/35788/>
- ⁵³ <https://qoshe.com/who>
- ⁵⁴ <https://qoshe.com/news>,
- <https://qoshe.com/gazete/new-eastern-outlook-en>
- ⁵⁵ <http://www.vijayvaani.com/>
- ⁵⁶ <http://www.vijayvaani.com/AuthorProfile.aspx?pid=887>,

<https://journal-neo.org/author/james-oneill/page/11/>,
<https://journal-neo.org/2020/03/27/devastating-revelations-about-the-truth-behind-the-destruction-of-mh17/>
⁵⁷ <http://www.vijayvaani.com/AuthorProfile.aspx?pid=738>,
<http://www.vijayvaani.com/ArticleDisplay.aspx?aid=5324>
⁵⁸ <http://www.vijayvaani.com/AuthorProfile.aspx?pid=386>
⁵⁹ <http://www.vijayvaani.com/AuthorProfile.aspx?pid=205>,
<https://www.theguardian.com/media/2011/jan/31/wikileaks-holocaust-denier-handled-moscow-cables>
⁶⁰ <https://www.newagebd.net/article/298/Opinion>,
<https://www.newagebd.net/credit/Yuriy%20Zinin>,
<https://www.newagebd.net/credit/Vladimir%20Terehov>,
<https://muckrack.com/viktor-mikhin>
⁶¹ <http://www.thefringenews.com/?s=new+eastern+outlook>
⁶² <http://www.thefringenews.com/about-us/>
⁶³ <https://countercurrents.org/author/peter-koenig/>
⁶⁴ <https://off-guardian.org/?s=christopher+black&submit=Search>,
<https://off-guardian.org/tag/james-oneill/>
⁶⁵ <https://www.veteranstopday.com/>
⁶⁶ <https://monitoring-bbc.co.uk/product/c20024k5>
⁶⁷ <https://www.globalresearch.ca/>
⁶⁸ <https://www.economist.com/united-states/2017/04/15/how-a-pair-of-self-publicists-wound-up-as-apologists-for-assad>
⁶⁹ <https://www.newsguardtech.com/wp-content/uploads/2020/03/GlobalResearch-ca-3-20-20.pdf>
⁷⁰ <http://www2.psych.utoronto.ca/users/furedy/Papers/af/wstd06.htm>
⁷¹ <https://www.globalresearch.ca/the-911-reader-the-september-11-2001-terror-attacks/5303012>
⁷² <https://www.theguardian.com/world/2002/apr/01/september11france>
⁷³ <https://web.archive.org/web/20171117193837/https://www.theglobeandmail.com/news/world/canadian-website-in-natos-sights-for-spreading-disinformation/article37015521/>
⁷⁴ <https://web.archive.org/web/20171117193837/https://www.theglobeandmail.com/news/world/canadian-website-in-natos-sights-for-spreading-disinformation/article37015521/>
⁷⁵ <http://www.slobodan-milosevic.org/news/smorg091304.htm>
⁷⁶ <https://www.globalresearch.ca/happy-birthday-fidel-castro/26009>
⁷⁷ <https://web.archive.org/web/20121026130610/http://www.4thmedia.org/aboutus/>,
<https://web.archive.org/web/20150516032538/http://www.4thmedia.org/aboutus/>
⁷⁸ <https://www.globalresearch.ca/author/finian-cunningham>
⁷⁹ <https://www.strategic-culture.org/news/2012/11/12/high-stakes-in-bahrain-repression/>,
<https://www.strategic-culture.org/contributors/?letter=C>
⁸⁰ <https://www.globalresearch.ca/author/pepe-escobar/page/5>,
<https://www.strategic-culture.org/contributors/pepe-escobar/>
⁸¹ <https://www.strategic-culture.org/contributors/federico-pieraccini/>
⁸² <https://www.globalresearch.ca/failed-turkish-coup-sabotage-incompetence-or-deception/5537479>
⁸³ <https://www.globalresearch.ca/author/federico-pieraccini>
⁸⁴ <https://www.globalresearch.ca/middle-east-in-turmoil-trump-netanyahu-and-mohammad-bin-salman-destroyers-of-the-neoliberal-world-order/5622748>
⁸⁵ <https://www.globalresearch.ca/protecting-chinas-belt-and-road-initiative-from-us-led-terrorism/5625448>
<https://www.strategic-culture.org/news/2018/01/09/protecting-belt-road-initiative-from-us-led-terrorism-will-china-send-troops-syria/>
⁸⁶ <https://southfront.org/a-terrorist-attack-against-eurasian-integration/>,
<https://www.geopolitica.ru/es/article/los-grandes-desarrollos-sugieren-fuertemente-el-fin-del-orden-unipolar-mundial>,
<https://sputniknews.com/politics/201607251043602692-turkey-erdogan-military-coup/>
⁸⁷ <http://www.globaltimes.cn/content/1133318.shtml>,
<https://qz.com/745577/inside-the-global-times-chinas-hawkish-belligerent-state-tabloid/>
⁸⁸ <https://www.globalresearch.ca/author/southfront/page/21>,
<https://web.archive.org/web/20150628083839/http://southfront.org/>
⁸⁹ <https://www.strategic-culture.org/web/20180308143532/https://www.strategic-culture.org/>
⁹⁰ <https://web.archive.org/web/20180314230228/https://www.strategic-culture.org/>
⁹¹ <https://web.archive.org/web/20171117193837/https://www.theglobeandmail.com/news/world/canadian-website-in-natos-sights-for-spreading-disinformation/article37015521/>
⁹² <https://medium.com/dfrlab/fakenews-made-in-china-576239152a84>,
<https://medium.com/@DFRLab>
⁹³ <https://twitter.com/zlj517/status/1238269193427906560>,
<https://twitter.com/zlj517/status/1238292025817968640>
⁹⁴ <https://www.wsj.com/articles/canadian-writer-fuels-china-u-s-tiff-over-coronaviruss-origins-11585232018>
⁹⁵ <https://www.globalresearch.ca/understanding-china/5695479>
⁹⁶ <https://www.globalresearch.ca/understanding-china/5695479>
⁹⁷ https://twitter.com/crg_crm?lang=en
⁹⁸ <https://www.globalresearch.ca/covid-19-coronavirus-a-fake-pandemic-whos-behind-it-global-economic-and-geopolitical-destabilization/5705063>
⁹⁹ <https://ecoterra.info/index.php/en/1671-covid-19-coronavirus-a-fake-pandemic>
¹⁰⁰ <https://jamaicapeacecouncil.wordpress.com/2020/03/08/covid-19-coronavirus-a-fake-pandemic-whos-behind-it-global-economic-social-and-geopolitical-destabilization-johns-hopkins-coronavirus-simulation-october-2019/>
¹⁰¹ <http://www.tlaxcala-int.org/article.asp?reference=28245>
¹⁰² <http://realtruthblog.com/current-quicklinx-3>
¹⁰³ <https://australiannationalreview.com/?s=chossudovsky>
¹⁰⁴ <https://southfront.org/fake-coronavirus-data-fear-campaign-spread-of-the-covid-19-infection/>
¹⁰⁵ <https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks>
¹⁰⁶ <https://rkn.gov.ru/mass-communications/reestr/media/p67382/?id=575587&page=67382>
¹⁰⁷ <https://www.rusprofile.ru/id/7601209>,
<https://news-front.info/contacts/>
¹⁰⁸ <https://novorosinform.org/402691>
¹⁰⁹ <https://news-front.info/>,
<https://news-front.info/about/>
¹¹⁰ <https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>
¹¹¹ <https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>,
<https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2Fdigital%2Finternet%2F2017-02%2Fbundesstag-elections-fake-news-manipulation-russia-hacker-cyberwar%2Fkomplettansicht>
¹¹² <https://www.rusprofile.ru/founders/10433419>,
https://www.znak.com/2016-07-05/kto_i_kak_poluchaet_prezidentskie_granty_dlya_nko_v_2016_godu
¹¹³ <https://time.com/4889471/germany-election-russia-fake-news-angela-merkel/>

114 <https://cfuv.ru/wp-content/uploads/2016/08/090203-opop-2017-o.pdf>

115 <https://news-front.info/about/>,

<https://news-front.info/2016/07/21/kak-dobrovolcy-nezavisimogo-agentstva-news-front-ispugali-professionalov-nemeckogo-gosudarstvennogo-telekanala-ard-konstantin-knyrik/>,

<https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>

116 <https://ru.krymr.com/a/27871931.html>,

<https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>,

<https://time.com/4889471/germany-election-russia-fake-news-angela-merkel/>,

<https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2Fdigital%2Finternet%2F2017-02%2Fbundestag-elections-fake-news-manipulation-russia-hacker-cyberwar%2Fkomplettansicht>

117 <https://medium.com/dfrlab/facebook-removes-propaganda-outlets-linked-to-russian-security-services-51f6e2f6b841>

118 <https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2Fdigital%2Finternet%2F2017-02%2Fbundestag-elections-fake-news-manipulation-russia-hacker-cyberwar%2Fkomplettansicht>

119 <https://euvsdisinfo.eu/disinformation-cases/?text=News+Front&date=&offset=130>

120 <https://euvsdisinfo.eu/report/coronavirus-was-spread-around-the-world-from-the-worldwide-us-biological-laboratories/>,

<https://de.news-front.info/2020/01/25/massenepidemie-in-china-coronavirus-eine-neue-entwicklung-aus-den-biolaboren-des-pentagon/>,

<https://news-front.info/2020/01/30/kitajskij-koronavirus-zastavil-vspomnit-o-sobytyah-na-ukraine-desyatiletnej-davnosti/>,

<https://euvsdisinfo.eu/report/us-tests-ethnic-weapons-against-slavs-in-its-biolabs-in-ukraine/>,

<https://en.news-front.info/2020/04/06/us-staged-coronavirus-terror-for-illegal-immigrants-migrants-plead-for-deportation/>,

<https://euvsdisinfo.eu/report/us-servicemen-imported-coronavirus-intentionally-into-china/>

121 <https://euvsdisinfo.eu/disinformation-cases/?text=News+Front&date=&offset=110>,

<https://euvsdisinfo.eu/disinformation-cases/?text=News+Front&date=&offset=70>,

<https://euvsdisinfo.eu/report/cia-ordered-puppet-zelenskyy-extend-sanctions-against-russian-social-media/>,

<https://euvsdisinfo.eu/report/more-than-1500-ukrainian-soldiers-in-donbas-are-infected-with-a-coronavirus/>,

<https://euvsdisinfo.eu/report/kyiv-stops-public-transport-nazis-are-patrolling-the-streets/>,

<https://euvsdisinfo.eu/report/an-ukrainian-terrorist-attack-was-perpetrated-in-the-us-a-situation-similar-to-the-2014-coup-in-kyiv/>

122 <https://euvsdisinfo.eu/report/eu-is-dead-it-is-incapable-to-take-control-over-the-coronavirus-crisis/>,

<https://euvsdisinfo.eu/report/the-coronavirus-epidemic-proves-that-the-eu-has-abandoned-ukraine/>,

<https://euvsdisinfo.eu/report/kyivs-western-protectors-are-inflaming-war-in-the-donbass/>,

<https://euvsdisinfo.eu/report/the-eu-provoked-a-civil-war-in-ukraine-now-it-destabilises-belarus/>

123 <https://euvsdisinfo.eu/report/nato-did-not-help-spain-fight-coronavirus/>,

<https://euvsdisinfo.eu/report/nato-does-not-care-about-montenegro-amid-covid-19-pandemic/>,

<https://euvsdisinfo.eu/report/nato-spreads-the-coronavirus-in-the-eu/%20%20E2%80%A2>

124 <https://news-front.info/2020/03/22/v-ssha-znali-o-gryadushhej-epidemii-davno/>,

<https://euvsdisinfo.eu/report/bill-gates-and-other-globalists-use-the-corona-pandemic-to-implant-microchips-in-the-whole-of-humanity/>,

<https://euvsdisinfo.eu/report/coronavirus-vaccines-big-pharma-fraud-bill-gates/>

125 <https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf>

126 <https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf>

127 <https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf>

128 <https://www.facebook.com/konstantin.knyrik/posts/550798279162508>

129 <https://www.youtube.com/channel/UCt94dhpYV06IMOTXcGxt3eQ>

130 https://www.mid.ru/en/foreign-policy/asset_publisher/zwl2FuDbhJx9/content/ob-udalenii-video-hostingom-youtube-akkauntov-telekanala-krym-24-informagentstv-anna-news-i-news-front-?_101_INSTANCE_zwl2FuDbhJx9_redirect=https%3A%2F%2Fwww.mid.ru%2Ffen%2Fdiverse%3Fp_id%3D101_INSTANCE_zwl2FuDbhJx9%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_pos%3D2%26p_p_col_count%3D6

131 https://twitter.com/News_Front_info/

132 <https://medium.com/dfrlab/facebook-removes-propaganda-outlets-linked-to-russian-security-services-51f6e2f6b841>

133 <https://isfed.ge/eng/blogi/saqartveloshi-politikuri-polarizatsiis-khelshemtskobi-rusuli-sainformatsio-operatsia-feisbuqze-da-masshi-chartuli-araavtenturi-angarishebi>

134 <https://news-front.info/konstantin-sergeevich-knyrik-biografiya/>

135 https://vk.com/knyrik?z=photo122769433_457248460%2Fphotos122769433

136 <https://www.youtube.com/watch?v=p0ws95DLwn8>

137 <https://www.zeit.de/zustimmung?url=https%3A%2F%2Fwww.zeit.de%2Fdigital%2Finternet%2F2017-02%2Fbundestag-elections-fake-news-manipulation-russia-hacker-cyberwar%2Fkomplettansicht>

138 <https://www.codastory.com/disinformation/armed-conflict/meet-the-kremlins-keyboard-warrior-in-crimea/>

139 <https://anton-shekhovtsov.blogspot.com/2014/08/pro-russian-extremists-in-2006-and-2014.html>,

<https://www.treasury.gov/press-center/press-releases/Pages/jj9993.aspx>

140 <https://www.youtube.com/watch?v=p0ws95DLwn8>

141 <http://anton-shekhovtsov.blogspot.com/2016/01/how-alexander-dugins-neo-eurasianists.html>

142 <https://www.rusprofile.ru/id/7601209> ,

<https://en.news-front.info/contact-us/> ,

<http://www.rodina.ru/novosti/V-Simferopole-proshla-konferenciya-regionalnogo-otdeleniya-vserossijskoj-politicheskoy-partii-Rodina-v-Respublike-Krym> ,

<https://www.thermoscowtimes.com/2012/09/30/rogozins-rodina-party-reinstated-a18170>,

<https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20140317.aspx>

143 <https://vk.com/knyrik?z=albums122769433> ,

<https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20140317.aspx>

<https://www.bloomberg.com/news/articles/2019-08-16/putin-s-iconoclastic-economics-guru-to-lose-kremlin-post>

144 <https://www.rusprofile.ru/founders/7601209>,

<https://www.kommersant.ru/doc/485775>

145 <https://ru.krymr.com/a/27871931.html>

146 <https://www.reg.ru/whois/?dname=southfront.org>

147 <https://koddos.net/>

148 <https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf>

149 <https://about.fb.com/wp-content/uploads/2020/05/April-2020-CIB-Report.pdf>

150 <https://southfront.org/antiwar-about-censorship-of-southfront-on-youtube-and-facebook/>

151 <https://novorosinform.org/402691>

152 <https://syrianfreepress.wordpress.com/about/#comment-30479>

153 <https://web.archive.org/web/20140307190510/https://www.youtube.com/user/crimeanfront>,

<https://web.archive.org/web/20140315135947/http://vk.com/crimeanfront>

154 <https://web.archive.org/web/20140625103752/http://krimfront.info/category/media/videogalereya/na-samom-dele/>

155 <https://web.archive.org/web/20140322200213/http://vk.com/crimeanfront>

156 <https://web.archive.org/web/20140803012046/http://vk.com/ygfront>,

<https://twitter.com/southfronteng>

157 <https://southfront.org/about-southfront/>
158 <https://southfront.org/about-southfront/>
159 <https://southfront.org/donate/>
160 <https://southfront.org/appeal-of-southfront-steering-committee-regarding-censorship-on-youtube-and-facebook/>
161 <https://maps.southfront.org/bellingcats-five-star-investigation-reveals-identity-of-southfront-founder/>,
<https://www.bellingcat.com/news/2019/09/30/pro-assad-lobby-group-rewards-bloggers-on-both-the-left-and-the-right/>
162 <https://southfront.org/appeal-of-southfront-steering-committee-regarding-censorship-on-youtube-and-facebook/>
163 <https://www.facebook.com/ViktorStoilovOfficial/> ,
<https://www.facebook.com/markademics>
164 <https://southfront.org/new-red-bloc-russian-chinese-alliance/>
165 <https://southfront.org/distraction-tactics-reports-of-chinese-and-iranian-hacking-russians-behind-protests/>
166 <https://southfront.org/how-and-why-the-us-government-perpetrated-the-2014-coup-in-ukraine/>
167 <https://southfront.org/documentary-on-mh17-reveals-5-year-long-string-of-lies/>
168 <https://southfront.org/another-step-towards-ukraine-like-scenario-for-belarus/>
169 <https://southfront.org/the-venezuela-iran-axis-of-unity-and-resistance-stands-the-test-of-time/>
170 <https://southfront.org/opcw-manipulated-chemical-weapons-report-on-syrias-douma-by-removing-critical-details/>
171 <https://southfront.org/russia-says-it-has-undeniable-evidence-that-militants-are-responsible-for-chemical-attack-on-aleppo/>
172 <https://southfront.org/russian-foreign-ministrys-comment-on-fifth-anniversary-of-crimeas-reunification-with-russia/>
<https://southfront.org/turkey-activates-certain-elements-of-s-400-anti-aircraft-missile-systems/>,
<https://southfront.org/two-new-disappointments-for-the-coup-planners-in-venezuela/>
173 <https://southfront.org/an-in-depth-look-behind-the-scenes-of-southfront-censorship/> ,
<https://euvsdisinfo.eu/south-front-russia-hiding-being-russian/> ,
<https://southfront.org/self-isolation-sobyanin-style-moscow-authorities-introduce-virus-quarantine-passes-draastically-limiting-freedoms-of-residents/>
174 <https://southfront.org/an-in-depth-look-behind-the-scenes-of-southfront-censorship/> ,
<https://english.khamenei.ir/news/4740/Iran-is-a-bright-and-shining-light-for-other-countries-to-follow>
175 <https://southfront.org/phenomena-of-coronavirus-crisis/>
176 <https://southfront.org/covid-19-the-fight-for-a-cure-one-gigantic-western-pharma-rip-off>
177 <https://southfront.org/the-coronavirus-covid-19-pandemic-the-real-danger-is-agenda-id2020/>
178 <https://southfront.org/usa-plan-militarized-control-of-population-the-national-covid-19-testing-action-plan/>
179 <https://southfront.org/finally-eu-blames-kremlin-disinformation-for-coronavirus-crisis/>
180 <https://southfront.org/covid-19-crisis-in-russia-lockdown-craziness-and-opposition-provocations/>
181 <https://southfront.org/an-in-depth-look-behind-the-scenes-of-southfront-censorship/>
182 <https://southfront.org/category/all-articles/products/maps/infographics/>,
<https://southfront.org/category/all-articles/products/maps/page/1/>,
<https://southfront.org/search/Military+Situation/>,
<https://southfront.org/category/southfront-tv/>
183 <https://www.youtube.com/channel/UCEV64LEWBVF0h48eUDxI96Q/featured>
184 <https://syrianfreepress.wordpress.com/about/#comment-27585>
185 <https://syrianfreepress.wordpress.com/about/#comment-30479>
186 <https://syrianfreepress.wordpress.com/about/#comment-30485>
187 <https://southfront.org/russian-foreign-ministry-finally-reacted-to-censorship-on-youtube-and-facebook/>
188 <https://www.geopolitica.ru/>
189 <https://www.eurozine.com/putins-brain/>
190 <https://www.foreignaffairs.com/articles/russia-fsu/2014-03-31/putins-brain>
191 <https://tec.fsi.stanford.edu/docs/aleksandr-dugins-foundations-geopolitics> ,
<https://www.eurozine.com/putins-brain/>
192 <https://www.eurozine.com/putins-brain/>
193 <https://tec.fsi.stanford.edu/docs/aleksandr-dugins-foundations-geopolitics>
194 <https://katehon.com/>
195 <https://rkn.gov.ru/mass-communications/reestr/media/p100/?id=337269&page=100>,
<https://web.archive.org/web/20121120174521/http://geopolitica.ru/>,
<https://web.archive.org/web/20171225083859/https://www.geopolitica.ru/>
196 <https://www.geopolitica.ru/en/mission>
197 <https://www.foreignaffairs.com/articles/russia-fsu/2014-03-31/putins-brain>
198 <https://foreignpolicy.com/2016/07/27/geopolitics-russia-mackinder-eurasia-heartland-dugin-ukraine- Eurasianism-manifest-destiny-putin/>
199 <http://anton-shekhovtsov.blogspot.com/2014/02/pro-russian-network-behind-anti.html>
200 <https://www.treasury.gov/press-center/press-releases/Pages/jl9993.aspx>
201 <http://cge.eurasia.org/about.shtml>,
<https://vk.com/neokons>
202 <https://www.geopolitica.ru/contact>,
<https://www.rusprofile.ru/history/10349103>
203 <https://www.geopolitica.ru/en/person/leonid-savin>
204 <https://www.rferl.org/a/greek-syria-deep-ties-russian- Eurasianist-dugin/26818523.html>
205 <https://www.treasury.gov/press-center/press-releases/Pages/jl9729.aspx>
206 <https://www.fondsk.ru/authors/leonid-savin-33.html>
207 <https://www.globalresearch.ca/author/leonid-savin>,
<https://rb.gy/x8nrdz>,
<https://rb.gy/ylendv>,
<https://rb.gy/vg0re8>,
<https://rb.gy/gakiku>
208 <https://rb.gy/wulcke>,
<https://www.geopolitica.ru/en/article/false-flag-operation-brussels> ,
<https://www.bbc.com/news/world-europe-35869985>
209 <https://rb.gy/r5qnny>,
<https://rb.gy/nfztel>,
<https://rb.gy/v7cvtx>
210 <https://www.geopolitica.ru/en/person/adomas-abromaitis>
<https://cyber.fsi.stanford.edu/io/publication/potemkin-think-tanks>
211 <https://www.geopolitica.ru/en/article/bill-gates-vaccinations-microchips-and-patent-060606>
212 <https://www.geopolitica.ru/it/article/la-russia-e-il-coronavirus>

213 <https://www.geopolitica.ru/en/article/new-malthusianism-and-misanthrope-dynasties>
214 <https://www.geopolitica.ru/en/article/coronavirus-and-hybrid-warfare>
215 <https://www.geopolitica.ru/en/news/former-putins-aide-coronavirus-us-biological-weapon>,
<https://www.theguardian.com/world/2014/mar/23/ukraine-crimea-what-putin-thinking-russia>
216 <https://www.geopolitica.ru/en/article/pandemic-service-globalization>,
217 <https://www.geopolitica.ru/node/73750>
218 <https://www.geopolitica.ru/en/article/pandemic-and-politics-survival-horizons-new-type-dictatorship>
219 <https://euvsdisinfo.eu/disinformation-cases/?text=geopolitica.ru&date=&offset=0>,
<https://euvsdisinfo.eu/report/the-western-world-is-dominated-by-a-handful-of-perverts-and-is-based-on-the-lies-of-woke-ideologies/>,
<https://euvsdisinfo.eu/report/the-genocide-of-the-russians-in-ukraine-began-in-2014-with-the-violation-of-the-rights-of-ukraines-russian-speaking-population/>,
<https://euvsdisinfo.eu/report/todays-western-males-are-feminized-semi-men-who-are-not-able-to-protect-their-women-raped-by-immigrants/>, <https://euvsdisinfo.eu/disinformation-cases/?text=geopolitica.ru&date=&offset=70>
220 <https://www.rusprofile.ru/founders/10349103>,
<https://www.rusprofile.ru/founders/7548034>,
https://tsargrad.tv/pervyi_russkij
221 <https://katehon.com/>
222 <https://katehon.com/ru>
223 <https://www.theguardian.com/world/2017/mar/06/russia-revolution-tsarist-school-moscow-nicholas-ii>,
https://tsargrad.tv/news/jeto-ne-piar-patriarh-kill-nazval-blagotvoritelnost-vizitnoj-kartochkoj-cerkvi_215548
224 https://tsargrad.tv/news/jeto-ne-piar-patriarh-kill-nazval-blagotvoritelnost-vizitnoj-kartochkoj-cerkvi_215548
225 <https://www.rbc.ru/rbcfreenews/553502619a79471f3e9554dd>,
<http://ligainternet.ru/en/liga/about.php>,
<https://meduza.io/en/feature/2017/07/27/the-kids-aren-t-alright>
226 <http://www.ligainternet.ru/upload/docs/liga-2016-v-17.pdf>,
<https://novayagazeta.ru/articles/2013/02/27/53718-tsenzor-151-dohodnoe-mesto>,
<http://en.kremlin.ru/catalog/persons/65/biography>,
<http://www.scrf.gov.ru/council/composition/>
227 <https://thebell.io/en/russia-s-orthodox-tycoon-is-bankrolling-a-monarchist-movement-but-where-does-he-get-his-money/>
228 <https://www.treasury.gov/press-center/press-releases/Pages/j9729.aspx>,
<https://www.wsj.com/articles/eu-places-sanctions-on-russian-oligarchs-1406749975>
229 https://tsargrad.tv/news/rossija-namerena-dekolonizirovat-afriku-zapad-vydavlivajat-s-chernogo-kontinenta_222972
230 <https://katehon.com/about-us>
231 <https://www.bloomberg.com/news/articles/2019-08-16/putin-s-iconoclastic-economics-guru-to-lose-kremlin-post>,
http://www.eurasiancommission.org/en/act/integr_i_makroec/Pages/default.aspx
232 <https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/20140317.aspx>
233 <http://council.gov.ru/en/structure/persons/303/>,
http://council.gov.ru/structure/commissions/iccf_def/#personnel
234 <https://riss.ru/profile/prime/>
235 <https://www.bbc.com/russian/features-39662290>,
<https://meduza.io/feature/2017/04/20/reuters-obvinil-rossijskiy-institut-strategicheskikh-issledovaniy-vo-vmeshatelstve-v-vybory-prezidenta-ssha-chem-etot-institut-zanimaetsya>
236 https://www.reuters.com/article/us-usa-russia-election-exclusive-idUSKBN17L2N3?feedType=RSS&feedName=topNews&utm_source=twitter&utm_medium=Social,
<https://www.wsj.com/articles/how-does-russia-meddle-in-elections-look-at-bulgaria-1490282352>
237 <https://riss.ru/analytics/26987/>
238 <https://www.fontanka.ru/2012/01/27/138/>
239 <https://www.rusprofile.ru/id/10349103>,
<http://fondsv.ru/about>
240 <https://dailystorm.ru/kultura/a-esli-ogon-ne-soydet>,
<https://www.foreignaffairs.com/reviews/capsule-review/2018-08-13/treacherous-path-insiders-account-modern-russia>
241 <http://fondsv.ru/media-article?slug=plita-groba-gospodna-novodel>,
<http://jerusalem-ippo.org/about/autors/?id=42>,
<https://katehon.com/person/mihail-yakushev>
242 <https://www.rusprofile.ru/id/11643625>
243 <https://web.archive.org/web/20191222123628/http://centrisi.com/en/home-2/>
244 <http://confidentielafrique.com/pouvoir-reseau/russie-afrique-centre-strategique-affaires-africaines-signe-protocole-centre-initiatives-strategique-international-de-moscou/>
245 <https://www.rusprofile.ru/person/grachev-ag-772270379404>,
<http://www.kremlin.ru/acts/bank/32687>,
<https://zatulin.ru/stenogramma-kruglogo-stola-komiteta-gosudarstvennoj-dumy-po-dela-m-sodruzhestva-nezavisimy-gosudarstv-i-svyazyam-s-sootchestvennikami-24-marta-2011g/>
246 <https://www.kyivpost.com/article/ukraine-politics/foreign-ministry-studying-reports-on-possible-expu-46152.html>
247 <https://www.unian.net/politics/394309-rossijskiy-genkonsul-pokidaet-odessu.html>
248 https://tsargrad.tv/news/bioinzheneriy-vsjo-rasskazhut-koronavirus-sozdan-rukotvorno-sergej-glazev_242768,
https://zavtra.ru/blogs/glaz_ev_raskol,
<https://nationalinterest.org/commentary/interview-sergey-glazev-10106>,
<https://books.google.com/books?id=FG-hDwAAQBAJ&pg=PA122&lpg=PA122&dq=sergey+glazev+conspiracy+theories&source=bl&ots=3XEG7wQbM&sig=ACfU3U3XjRGIKWh9UIYH9GOWkHelMmdL-A&hl=en&sa=X&ved=2ahUKEwjXU6xtKzPAhUt98KHWIRBdc4ChDoATAlegQICAB#v=onepage&q=sergey%20glazev%20conspiracy%20theories&f=true>
249 https://aif.ru/politics/world/leonid-reshetnikov_ssha_visyat_na_voloske?utm_source=infox_sg
250 https://ruskline.ru/opp/2015/4/8/civilizaciya_rossiya
251 <https://tjournal.ru/analysis/110993-senator-klimov-delaet-gromkie-zayavleniya-po-lyubomu-povodu-kto-on-takoy-i-pochemu-boitsya-vashingtonskih-podstrekateljev?from=yan-dex>
252 <https://tjournal.ru/analysis/110993-senator-klimov-delaet-gromkie-zayavleniya-po-lyubomu-povodu-kto-on-takoy-i-pochemu-boitsya-vashingtonskih-podstrekateljev?from=yan-dex>
253 <https://novayagazeta.ru/articles/2017/07/13/73101-ofshory-na-glazah>
254 <https://euvsdisinfo.eu/disinformation-cases/?text=katehon&date=&offset=10>
255 <https://katehon.com/person/adomas-abromaitis>,
<https://fsi-live.s3-us-west-1.amazonaws.com/s3fs-public/potemkin-pages-personas-sio-wp.pdf>
256 <https://katehon.com/>
257 <https://web.archive.org/web/20150327063341/http://katehon.com/>
258 <https://www.nationalreview.com/2014/06/wrong-right-robert-zubrin/>,
<https://theins.ru/politika/2113>
259 https://www.youtube.com/watch?v=hf6K6pjK_Yw,

https://www.bellingcat.com/news/uk-and-europe/2017/03/04/kremlins-balkan-gambit-part/
²⁶⁰ https://www.bellingcat.com/news/uk-and-europe/2017/03/25/balkan-gambit-part-2-montenegro-zugzwang/,
https://www.fpri.org/wp-content/uploads/2018/07/kraemer-rfp5.pdf
²⁶¹ https://www.nytimes.com/2017/04/20/world/europe/putin-trump-election-kremlin.html
²⁶² https://www.rferl.org/a/bulgaria-charges-former-lawmaker-with-spying-for-russia/30157289.html
https://www.rferl.org/a/russian-oligarch-malofeyev-banned-bulgaria-10-years-spy-scandal/30159179.html,
https://www.rferl.org/a/bulgarian-accused-of-spying-awarded-russia-s-order-of-friendship/30252738.html
²⁶³ https://www.geopolitica.ru/en/article/ideological-platform- Eurasian-movement,
https://archive.li/6ijl,
https://www.ft.com/content/27125702-71ec-11e5-ad6d-f4ed76f0900a
²⁶⁴ https://www.bellingcat.com/news/uk-and-europe/2019/09/03/lega-nords-bedfellows-russians-offering-illicit-funding-to-italian-far-right-party-identified/,
https://theins.ru/politika/2113
²⁶⁵ https://www.treasury.gov/press-center/press-releases/Pages/j19993.aspx
²⁶⁶ https://www.theguardian.com/world/2015/apr/07/anonymous-international-hackers-kremlin,
https://cgrozev.wordpress.com/2017/01/02/would-you-like-fries-with-that-conspiracy/
²⁶⁷ https://cgrozev.files.wordpress.com/2017/01/the-extreme-right-in-europe.pdf
²⁶⁸ https://cgrozev.wordpress.com/2017/01/02/would-you-like-fries-with-that-conspiracy/
²⁶⁹ https://theins.ru/politika/2113,
http://argumentua.com/stati/instrumenty-kremlia-eksklyuzivnyi-spisok-agentov-rossiiskogo-vliyaniya-v-evropeiskikh-stranakh
²⁷⁰ https://cgrozev.wordpress.com/2017/01/02/would-you-like-fries-with-that-conspiracy/,
https://books.google.com/books?id=1rA0DwAAQBAJ&pg=PT191&pg=PT191&dq=Katehon+France&source=bl&ots=vfPDY05h7R&sig=ACfU3U0L2qWxQM0SCv_ E0n9kmlWtsuAYg&hl=en&sa=X&ved=2ahUKewjA_ZGE3CdpAhVjmHIEHCD-Cv84ChDoATADEgQIChABv=onepage&q=Katehon%20France&f=false
²⁷¹ The GEC used an in-house online media analysis tool to analyze all content published by the following sites during the specified time period: Global Research (globalresearch.ca, mondialisation.ca, globalization.ca), News Front (news-front.info, en.news-front.info, bgr.news-front.info, de.news-front.info, es.news-front.info, sr.news-front.info, fr.news-front.info, hu.news-front.info, ge.news-front.info, sk.news-front.info), SouthFront (southfront.org, de.southfront.org, ru.southfront.org), Geopolitica.ru (geopolitica.ru), The Strategic Culture Foundation (strategic-culture.org), New Eastern Outlook (journal-neo.org, ru.journal-neo.org), and Katehon (katehon.com)
²⁷² SimilarWeb potential readership is defined as the number of people who potentially saw an article based on the number of unique visitors to the publication's website
²⁷³ https://southfront.org/indestructible-kalashnikov-expert-tries-fails-to-destroy-wwii-pssh-41-submachine-gun-video/,
https://www.globalresearch.ca/russian-indian-oil-deal-unpleasant-surprise-iran-not-us/5703466,
https://www.globalresearch.ca/leaked-docs-point-no-buk-missile-systems-around-mh17-crash-area-dutch-journo-reveals/5703997,
https://www.globalresearch.ca/historic-constitutional-changes-russia/5717576,
https://en.news-front.info/2020/03/19/ukraine-is-preparing-a-provocation-in-the-crimea-zakharova/
²⁷⁴ https://ru.journal-neo.org/2020/02/20/biologicheskaya-vojna-ssha-protiv-kitaya/,
https://journal-neo.org/2020/02/20/us-wages-biological-war-against-china/
²⁷⁵ https://bgr.news-front.info/2020/02/22/biologichnata-vojna-na-sashh-sreshhu-kitaj/
²⁷⁶ https://www.rt.com/news/482405-iran-coronavirus-us-biological-weapon/,
https://www.globalresearch.ca/%d1%81oronavirus-product-us-biological-attack-aimed-iran-china-irgc-chief-claims/5705747,
https://de.news-front.info/2020/03/09/coronavirus-aus-den-weltweiten-us-biolaboren-in-die-welt-verbreitet/
²⁷⁷ https://www.globalresearch.ca/covid-19-wuhan-virus-cia-biological-warfare-cuba/5706466,
https://www.globalresearch.ca/beijing-believes-covid-19-biological-weapon/5706558
²⁷⁸ https://bgr.news-front.info/2020/03/20/biolaboratoriyata-na-sashh-v-gruziya-zaplaha-za-koronavirusa-ili-za-horata/
²⁷⁹ https://www.globalresearch.ca/video-turkish-drones-falling-idlib-moderate-rebels-gas-themselves-mistake/5705709
²⁸⁰ https://www.globalresearch.ca/30-mila-soldati-dagli-usa-in-europa-senza-mascherina/5705348,
https://www.mondialisation.ca/30-mille-soldats-arrivent-des-usa-en-europe-sans-masque/5642335,
https://www.globalresearch.ca/30000-u-s-soldiers-sent-into-europe-without-masks/5706084
²⁸¹ https://journal-neo.org/2020/02/25/defexpo-india-2020-military-cooperation-between-russia-and-india-is-as-good-as-ever/,
https://ru.journal-neo.org/2020/02/25/defexpo-india-2020-rossijsko-indijskoe-vts-ne-oslabevat/
²⁸² https://bgr.news-front.info/2020/03/21/der-standard-rusija-dejstva-po-reshitelno-v-borbata-sreshhu-koronavirusa-otkolkoto-es/,
https://de.news-front.info/2020/03/21/der-standard-russland-hat-wirksamer-auf-die-ausbreitung-des-coronavirus-als-europa-reagiert/
²⁸³ https://southfront.org/escalation-or-de-escalation-prospects-of-russian-turkish-idlib-agreement/,
https://de.southfront.org/escalation-oder-de-eskalation-perspektiven-des-russisch-turkischen-idlib-abkommens/
²⁸⁴ https://es.news-front.info/2020/03/29/infierno-en-nueva-york-una-muerte-por-coronavirus-cada-17-minutos-los-medicos-no-pueden-seguir-el-ritmo/,
https://www.reddit.com/r/HongKong/comments/fhu9ij/coronaviruscovid19_originated_outside_china/,
https://theduran.com/chinas-coronavirus-a-shocking-update-did-the-virus-originate-in-the-us/
²⁸⁵ https://es.news-front.info/2020/03/29/infierno-en-nueva-york-una-muerte-por-coronavirus-cada-17-minutos-los-medicos-no-pueden-seguir-el-ritmo/
²⁸⁶ https://news-front.info/2020/02/24/golos-mordora-es-prekrashhaet-kormit-pribaltijskih-tigrov/
²⁸⁷ https://bgr.news-front.info/2020/04/04/11-ruski-samoleta-kaczaha-v-srbiya-v-pomoshh-za-borbata-sreshhu-koronavirusa/
²⁸⁸ https://bgr.news-front.info/2020/04/06/smi-zhitelite-na-krim-sa-uveren-iche-rusija-shhe-izdrzhi-na-natsika-na-sankcii/
²⁸⁹ https://southfront.org/russian-airstrike-kills-senior-al-qaeda-commander-in-western-aleppo/
²⁹⁰ https://www.strategic-culture.org/news/2020/05/29/german-official-leaks-report-denouncing-corona-as-global-false-alarm/
²⁹¹ https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2020/05/mitarbeiter-bmi-verbreitet-privatmeinung-corona-krisenmanagement.html?sessionid=4DC42CAAFEB4B7F0B2CEF08B8EEC12F0_1_cid364
²⁹² https://deutsch.rt.com/inland/102396-umstrittene-bmi-analyse-wissenschaftler-kritisieren/
²⁹³ https://healthfeedback.org/claimreview/german-ministry-employee-makes-unsupported-claim-that-covid-19-pandemic-is-a-global-false-alarm-in-widely-circulated-yet-unsolicited-opinion-article/,
https://www.spiegel.de/international/germany/berlin-fears-populists-will-exploit-protest-movement-a-3a4702b8-6701-401d-b712-6d3e19453a56
²⁹⁴ https://www.globalresearch.ca/greater-israel-the-zionist-plan-for-the-middle-east/5324815
²⁹⁵ https://www.globalresearch.ca/hospitals-getting-paid-more-label-cause-death-coronavirus/5709720
²⁹⁶ https://www.globalresearch.ca/mass-sterilization-kenyan-doctors-find-anti-fertility-agent-in-un-tetanus-vaccine/5431664
²⁹⁷ https://news-front.info/2020/04/14/aleksandr-rodzhers-predavshie-rodinu-teryayut-talant/#XpWnN9IzfO9 twitter
²⁹⁸ https://es.news-front.info/2020/01/06/periodista-sueco-palestino-muere-justo-antes-de-exponer-a-soros-y-aschberg/
²⁹⁹ https://es.news-front.info/2020/03/31/corte-suprema-de-brasil-pide-suspender-a-bolsonaro-180-dias-por-su-ineficiencia-contr-el-coronavirus/#XoRbFgfwmr4 twitter
³⁰⁰ https://southfront.org/the-coronavirus-covid-19-pandemic-the-real-danger-is-agenda-id2020/
³⁰¹ https://southfront.org/southfronts-youtube-channel-is-banned/
³⁰² https://southfront.org/u-s-used-601m-seized-from-venezuela-to-fund-border-wall-with-mexico/
³⁰³ https://www.strategic-culture.org/news/2020/05/29/german-official-leaks-report-denouncing-corona-as-global-false-alarm/
³⁰⁴ https://www.strategic-culture.org/news/2020/04/30/is-it-time-to-launch-an-investigation-into-the-bill-melinda-gates-foundation-for-possible-crimes-against-humanity/
³⁰⁵ https://www.strategic-culture.org/news/2020/04/21/what-did-us-intel-really-know-about-chinese-virus/
³⁰⁶ https://www.geopolitica.ru/en/news/putin-95-world-terrorist-attacks-are-made-cia

³⁰⁷ <https://www.geopolitica.ru/es/news/ingenieria-social-el-mundialista-soros-quiere-abortos-en-todo-el-planeta>
³⁰⁸ <https://www.geopolitica.ru/es/article/antifascistas-el-ejercito-del-terror-de-los-globalistas>
³⁰⁹ <https://journal-neo.org/2020/05/20/why-is-trump-drumbeating-a-new-cold-war-with-china/>
³¹⁰ <https://journal-neo.org/2020/04/15/the-remarkable-doctor-a-fauci/>
³¹¹ <https://katehon.com/it/article/chi-e-enrico-sassoon-padrino-di-casaleggio-associati-e-movimento-5-stelle>
³¹² <https://katehon.com/article/hub-world-evil-british-deep-state>
³¹³ <https://katehon.com/1310-europe-on-the-eve-of-the-civil-war.html>



GEC Special Report:

Pillars of Russia's Disinformation and Propaganda
Ecosystem

DEFENDANTS' EXHIBIT 143:

MARCH 03, 2023

EXECUTIVE SUMMARY: Initial Blueprint for the White House Task Force to Address Online Harassment and Abuse

Online harassment and abuse is increasingly widespread in today's digitally connected world. This can include online threats and intimidation as well as various forms of technology-facilitated gender-based violence (GBV), such as the non-consensual distribution of intimate images, cyberstalking, and sextortion. Women, girls, and LGBTQI+ individuals are disproportionately affected. Survivors of online harassment and abuse—especially image-based abuse—are often forced to relive their trauma and face ongoing harm that increases exponentially over time, owing to the viral flow of information on digital media and the difficulty of removing damaging, non-consensual content. Simply put: the scale, reach, and amplification effects of technology platforms have exacerbated GBV, and platforms have not sufficiently prevented or addressed how these modalities are used for harm.

To tackle this scourge, President Biden issued a Presidential Memorandum in June 2022 establishing the White House Task Force to Address Online Harassment and Abuse (Task Force), with a mandate to develop concrete actions in a Blueprint to prevent online harassment and abuse, provide support for survivors, increase accountability, and expand research.

Since its launch, the Task Force has heard from hundreds of stakeholders—survivors, advocates, parents, educators, law enforcement, medical and legal professionals, and researchers—who discussed the significant harm caused by online harassment and abuse. The powerful testimonies of survivors, including from youth, college students, public figures, and social media influencers, demonstrate the widespread reach of technology-facilitated GBV. While each of their stories is unique, they share common threads and lessons that informed the initial Task Force Blueprint.

Stakeholders shared with the Task Force how online harassment and abuse can have a severe impact on health, disrupt education, and derail careers. They explained how victims experience real, devastating consequences to their health, including post-traumatic stress disorder (PTSD), depression, anxiety, eating disorders, self-harm, and suicide, as well as increased risk of physical and sexual violence. Survivors described how they self-censored and

withdrew from online spaces and from broader engagement in academic, workplace, or social settings, often encouraged to do so by those who were unable—or unwilling—to help. The Task Force also heard from stakeholders about the impact on safety, health and wellbeing of children and youth stemming from the proliferation of child sexual abuse material traded online—including through exposure to unknown adults through gaming and messenger platforms.

The stakes of inaction couldn't be higher: experts from a range of disciplines underscored to the Task Force that in addition to the devastating effects on individuals, the proliferation of online harassment, abuse and misogyny results in the normalization of this abusive behavior and the degradation of our democracy and public safety, including through the suppression and silencing of diverse voices, and the violent expression of gender-motivated, extremist acts. Despite the pervasive nature of online harassment and abuse, as well as robust evidence of its consequences, it became evident to the Task Force that there is much more to be done to ensure that educators, parents, service providers, the legal system, and society as a whole are aware of and responsive to the issue and its detrimental impacts.

Today, the Biden Harris Administration is releasing an Executive Summary of the initial Task Force Blueprint, which includes a broad range of new and expanded commitments from Federal agencies to address technology-facilitated GBV across four main lines of effort: Prevention, Survivor Support, Accountability, and Research. Through this Blueprint, Senior Administration officials are working to operationalize the President's call to action in the State of Union for solutions to address online safety, health, privacy, and accountability. While the President continues to call on Congress to do its part, senior officials from Federal departments and agencies are undertaking key actions across the Administration.

The following are highlights from the initial Blueprint developed by the Task Force:

Prevention, including actions to create safer online environments for youth and adults, incorporate digital safety curricula into our schools, and provide resources and trainings for parents, educators, and employers, such as:

- **Promoting Prevention through Digital Equity Grants.** The National Telecommunications and Information Administration of the Department of Commerce plans to promote prevention efforts and increase awareness of services and support for victims of online harassment and abuse through the forthcoming Notice of Funding Opportunity for the FY24 Digital Equity Competitive Grant Program, which can provide support to digital inclusion projects that address online safety, and work to prevent online

harassment and abuse, in order to ensure that all people and communities have the skills, technology, and capacity needed to reap the full benefits of our digital economy.

Survivor Support, including efforts to increase training and technical assistance to law enforcement, prosecutors, educators, and victim advocates, so that survivors can access support and assistance from professionals who recognize the complexities and seriousness of technology-facilitated gender-based violence, such as:

- **New Resources to Train Law Enforcement, Prosecutors, and Victim Services Providers on Cybercrimes against Individuals.** The Consolidated Appropriations Act of 2023 (FY23 omnibus law) allocates \$7 million for the Department of Justice (DOJ) to fund two new programs authorized in the Violence Against Women Act reauthorization of 2022 (VAWA), including the establishment of a National Resource Center on Cybercrimes Against Individuals, and grants to provide training and support to State, Tribal, and local law enforcement, prosecutors, and judicial personnel to assist victims of cybercrimes. Cybercrimes is defined in VAWA as the use of electronic interactive devices to harass, threaten, stalk, extort, coerce, cause fear to, or intimidate an individual, or without consent distribute intimate images of an adult.

Accountability, including strengthening coordination among Federal, state, Tribal, territorial and local law enforcement agencies to investigate and prosecute cyberstalking, image-based abuse, sextortion, and child sexual exploitation online, and providing resources for workplaces and schools to hold individuals accountable for engaging in online harassment and abuse, such as:

- **Guidance to Institutions of Higher Education on Clery Act Obligations regarding Online Harassment and Abuse.** The Department of Education will issue guidance to help institutions comply with the Clery Act and educate students and employees about their rights and options under the law. This forthcoming guidance will clarify that certain acts of online harassment and abuse, including the non-consensual distribution of intimate images, are reportable offenses under the Clery Act when they occur as part of a pattern of cyberstalking and for hate crimes that are classified as acts of intimidation.
- **New Initiative for the Prosecution and Investigation of Online Abuse.** DOJ's Office on Violence Against Women will launch an initiative, with the funding allocated in the FY 23 bipartisan omnibus, focused on the prosecution and investigation of online abuse.

Research, to inform evidence-based interventions, deepen our understanding of the impacts of exposure to online harassment and abuse, including mental health implications for youth

and adults, and guide upstream efforts to prevent young men and boys from engaging in targeted acts of violence that share roots with online misogyny and other forms of hate, such as:

- **Research on Online Harassment, Abuse, and Youth Social and Emotional Development.** The National Institutes of Health (NIH) will host a scientific workshop to identify gaps and challenges in advancing the research agenda on online harassment and abuse, and continue to support investigator-initiated research to better understand the clinical and developmental implications of online harassment and abuse, including child sexual exploitation and sextortion. This will complement efforts by NIH to implement the bipartisan Children and Media Research Advancement Act (CAMRA), passed by Congress in the bipartisan omnibus law, which directs \$15 million in the first of a multi-year initiative for NIH to research technology and media's effects on infants, children, and adolescents in core areas of cognitive, physical, and socio-emotional development.

Other recent actions to address online harassment and abuse include:

- **Supporting Survivors of Technology-Facilitated Abuse to Separate from their Abusers' Mobile Phone and Wireless Accounts.** In February, the Federal Communications Commission (FCC) proposed rules to implement key provisions in the recently enacted Safe Connections Act to support survivors of domestic abuse and other related crimes seeking to maintain critical connections with friends, family, and support networks. These proposed rules would help survivors obtain separate service lines (through their mobile phones and broadband plans) from shared accounts that include their abusers, protect the privacy of calls made by survivors to domestic abuse hotlines, and provide support for survivors who suffer from financial hardship through the FCC's affordability programs.
- **Advancing Research on Targeted Violence, Exploring its Nexus with Misogyny, Online Harassment, and Domestic Violence.** Earlier this month, the U.S. Secret Service's National Threat Assessment Center (NTAC), under the Department of Homeland Security, released Mass Attacks in Public Spaces: 2016 – 2020, a comprehensive report examining 173 incidents of targeted violence and highlighting the observable commonalities among the attackers. The report reinforces NTAC's prior research demonstrating that individuals who perpetrate acts of targeted violence frequently display histories of concerning behavior, including hate-based beliefs, domestic violence, harassment, and threatening online communications.

- **Holding Gaming Platforms Accountable Under the Federal Trade Commission's**

Authority. In December 2022, the Federal Trade Commission settled two actions against Epic Games, Inc., creator of the popular video game Fortnite, requiring the company to pay a total of \$520 million in relief over allegations it violated the Children's Online Privacy Protection Act (COPPA), and employed dark patterns—design practices to intentionally manipulate users—to charge consumers without authorization. In a first-of-its-kind provision, the settlement also requires Epic to adopt strong privacy default settings for children and teens, ensuring that voice and text communications are turned off by default, in order to reduce the risk of matching children and teens with adult strangers. In a complaint filed in federal court, the FTC alleged that Epic violated the COPPA Rule by collecting personal information from children under 13 who played Fortnite, a child-directed online service, without notifying their parents or obtaining their parents' verifiable consent. Epic also allegedly violated the FTC Act's prohibition against unfair practices by enabling real-time voice and text chat communications for children and teens by default, exposing them to dangerous and psychologically traumatizing issues such as suicide, as well as bullying, threats and harassment.

- **Preventing and Addressing Technology-Facilitated Gender-Based Violence Globally.**

In December 2022, the Administration released an updated U.S. Strategy to Prevent and Respond to Gender-Based Violence Globally, which bolsters U.S. commitments to prevent and address this global scourge, including a specific objective to prevent and respond to technology-facilitated gender-based violence. The Strategy complements the Administration's ongoing efforts to better prioritize, understand, prevent, and address technology-facilitated gender-based violence through the Global Partnership for Action on Gender-Based Online Harassment and Abuse, which the U.S. launched in 2022 and coordinates with 11 other countries.

Over the next year, the Task Force will work across key federal agencies to build on the initial Blueprint for Action, and will release a final report at the end of the year. The Biden-Harris Administration recognizes online harassment and abuse as a multifaceted problem requiring a multifaceted response. As an Administration, we will continue to harness the whole of government to address it, as a matter of gender equity and equality, national security, and technology accountability. We will therefore continue to pursue meaningful actions to address online harassment and abuse in all its forms, recognizing that bolstering online safety requires coordination and accountability across sectors, spanning Federal, state, Tribal, territorial and local governments, community-based organizations, schools, and the private sector, including the tech sector.

DEFENDANTS' EXHIBIT 144:



[Back to Newsroom](#)

[Meta](#)

Keeping People Safe and Informed About the Coronavirus

December 18, 2020

By Kang-Xing Jin, Head of Health

[*Jump to latest news*](#)

Summary

Facebook is supporting the global public health community's work to keep people safe and informed during the coronavirus public health crisis. We're also working to address the long-term impacts by supporting industries in need and making it easier for people to find and offer help in their communities.

Here's an overview of how we're providing access to accurate information, supporting relief efforts and keeping people connected. We'll continue to add to this post as we announce updates.

1. Ensuring everyone has access to accurate information and removing harmful content

- Connecting people to credible information on Facebook, Messenger, Instagram and WhatsApp
- Combating COVID-19 misinformation across our apps
- Investing \$100 million in the news industry and supporting fact-checkers
- Prohibiting exploitative tactics in ads and banning ads for medical face masks, hand sanitizer, disinfecting wipes and COVID-19 test kits

2. Supporting health and economic relief efforts

- Matching \$20 million in donations to support COVID-19 relief efforts and donating \$25 million to support healthcare workers on the front line
- Investing \$100 million in small businesses and making it easier for people to support their local businesses
- Supporting global health organizations with free ads and more
- Empowering partners with data and tools

3. Keeping people connected

- Making it easier for people to request or offer help in their communities
- Helping local governments and emergency health organizations reach people on Facebook and Messenger, and collaborate using Workplace for free
- Sharing well-being tips and resources and donating \$2 million to support mental health crisis helplines
- Keeping our apps stable and reliable

Latest News

Update on December 18, 2020 at 4:00AM PT:

Updating Our Ad Policy for COVID-19 Vaccines

Given the recent approval of COVID-19 vaccines, we want people to be able to safely promote information about these vaccines on Facebook. We will now allow ads that highlight the ability of a COVID-19 vaccine to prevent someone from contracting the virus, as well as ads promoting ways to safely access a COVID-19 vaccine. We'll continue to prohibit content that tries to exploit the pandemic for commercial gain. And ads or organic posts that promote the sale of a COVID-19 vaccine, such as attempts to sell COVID-19 vaccine kits or expedited access to the vaccine, will be rejected. We will also reject ads that claim the vaccine is a cure for the virus.

It will take some time to train our systems and teams on these policies, and we expect enforcement to ramp up over the coming weeks and months.

Update on December 11, 2020 at 10:00AM PT:

Providing Aid to Diverse Suppliers through Receivables Financing

In response to the ongoing impact of the COVID-19 pandemic – particularly the challenges facing minority and women-owned businesses – we recently launched The Facebook Receivables Financing Program to support US-based suppliers. This one-year financing program allows minority, women, veteran, LGBTQ and disability-owned companies that are headquartered in the US and have been paid directly by Facebook in 2019 or 2020 to have their invoices paid now instead of in the 60 to 120 day period it normally takes to get paid for work they've already done. Our goal with this program is to help level the playing field by providing businesses with access to more working capital.

We'll do this by providing immediate cash for work suppliers have done and pay they're owed by other, non-Facebook, companies. Suppliers can upload eligible invoices to the Receivables Financing platform and get funded in a few days. We partnered with Supplier Success, a minority-owned business with extensive experience providing receivables financing, to administer our Receivable Financing platform and collaborated with Crowdz.io to operate a seamless and secure platform to safely buy receivables. Together, Supplier Success and Crowdz.io will collect the suppliers' invoices from their customers, and Facebook will reinvest the collected receivables to purchase additional invoices. Facebook is not making any return on these funds.

Removing False Claims About COVID-19 Vaccines

Given the recent news that COVID-19 vaccines will soon be rolling out around the world, over the coming weeks we will start removing false claims about these vaccines that have been debunked by public health experts on Facebook and Instagram. This is another way that we are applying our policy to remove misinformation about the virus that could lead to imminent physical harm. This could include false claims about the safety, efficacy, ingredients or side effects of the vaccines. For example, we will remove false claims that COVID-19 vaccines contain microchips, or anything else that isn't on the official vaccine ingredient list. We will also remove conspiracy theories about COVID-19 vaccines that we know today are false: like specific populations are being used without their consent to test the vaccine's safety. We will not be able to start enforcing these policies overnight. Since it's early and facts about COVID-19 vaccines will continue to evolve, we will regularly update the claims we remove based on guidance from public health authorities as they learn more.

We will also continue to help people stay informed about these vaccines by promoting authoritative sources of information through our [COVID-19 Information Center](#).

Update on November 30, 2020 at 3:00PM PT:

Mark Zuckerberg is live with Dr. Anthony Fauci, America's top infectious disease expert, to discuss progress toward a COVID-19 vaccine and how we can slow the spread of the virus this holiday season.



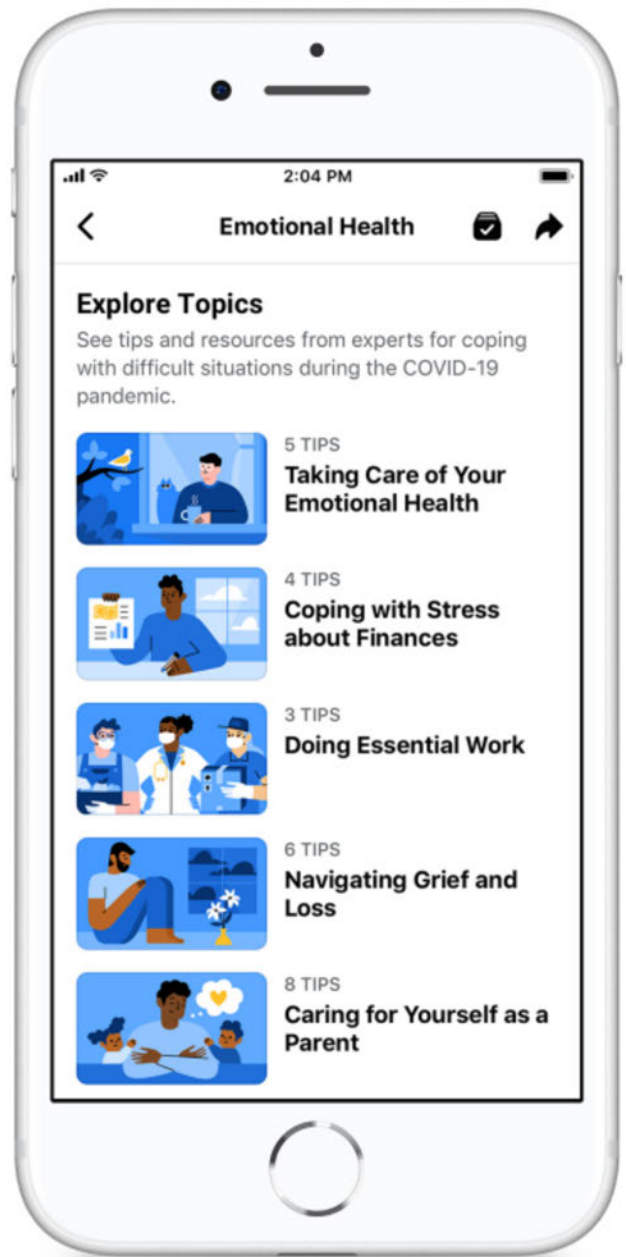
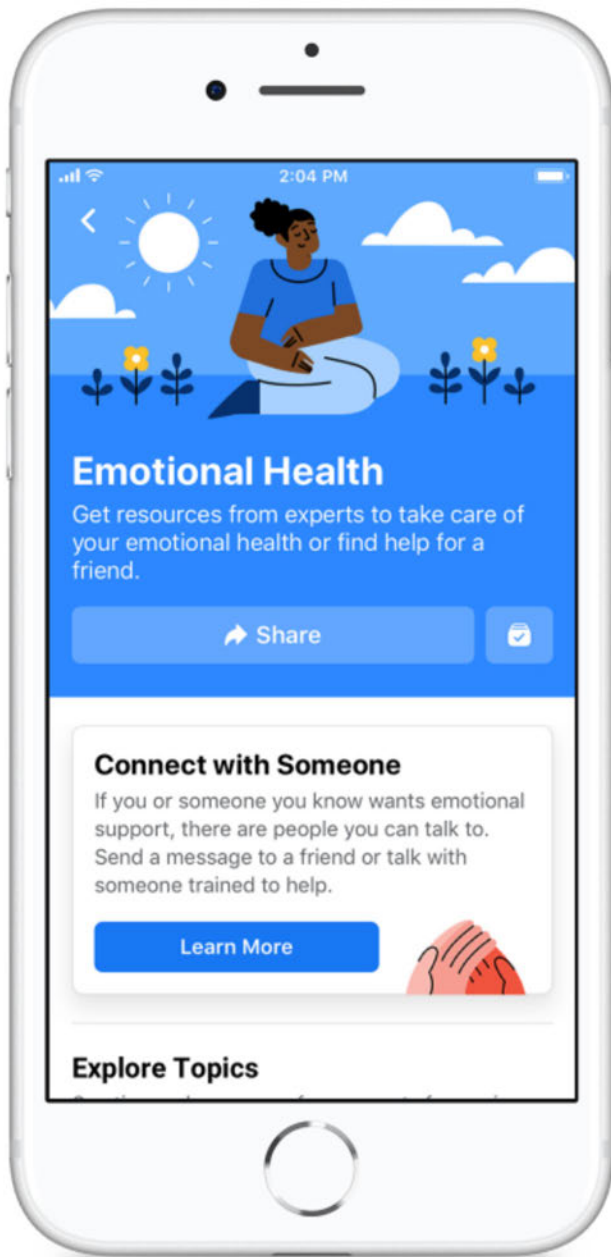
Mark Zuckerberg was live

Share

Connecting People to Mental Health Resources

Experts agree that COVID-19 has exacerbated mental health challenges around the world, and the repercussions will be felt for years to come. We’ve been working with leading authorities around the world — like NAMI, Kids Help Phone and It’s OK to Talk — to invest in the critical areas of mental health support, including handling financial stress, parenting support, coping with loss and grief, managing substance use and taking care of overall emotional health. Today we’re introducing Emotional Health, a centralized resource center on the Facebook app with tips and information from leading experts. The resource will be available globally, with locally relevant information from mental health officials.

Learn more about how we’re making it easier for people to get the support they need for themselves and others who might be struggling.



Update on August 19, 2020 at 10:05AM PT:

Allowing the Promotion and Sale of Hand Sanitizer and Surface Disinfecting Wipes

In March, we temporarily banned ads and commerce listings for hand sanitizer and surface disinfecting wipes to help protect against scams, inflated prices and hoarding. Since then, we've continued to monitor trends and activity around COVID-19 to better understand how people are using our platform and advertising tools during the pandemic. Today we're scaling back this temporary ban to allow people to promote and trade hand sanitizer and surface disinfecting wipes on our apps.

Update on August 17, 2020 at 7:40AM PT:

Supporting Teachers, Parents and Students This Back-To-School Season

Back-to-school looks different this year due to COVID-19, and parents, teachers and students around the world are facing a myriad of challenges, from remote teaching and learning, balancing work and home responsibilities, and most importantly, maintaining the safety and well-being of everyone involved. To help, we're launching an Educator Hub to support teachers and providing resources across our apps to help people stay connected and take care of each other. The Educator Hub will help teachers find or build their online communities and discover guides and other resources for the classroom and beyond. [Learn more.](#)

Update on July 16, 2020 at 2:02PM PT:

Mark Zuckerberg is live with Dr. Anthony Fauci, America's top infectious disease expert. They'll discuss the US' response to COVID-19, progress on a vaccine, and what we need to do next to stop the spread of the virus.



Live with Dr. Fauci, the nation's top infecti...

Mark Zuckerberg was live

Share

Facebook Watch

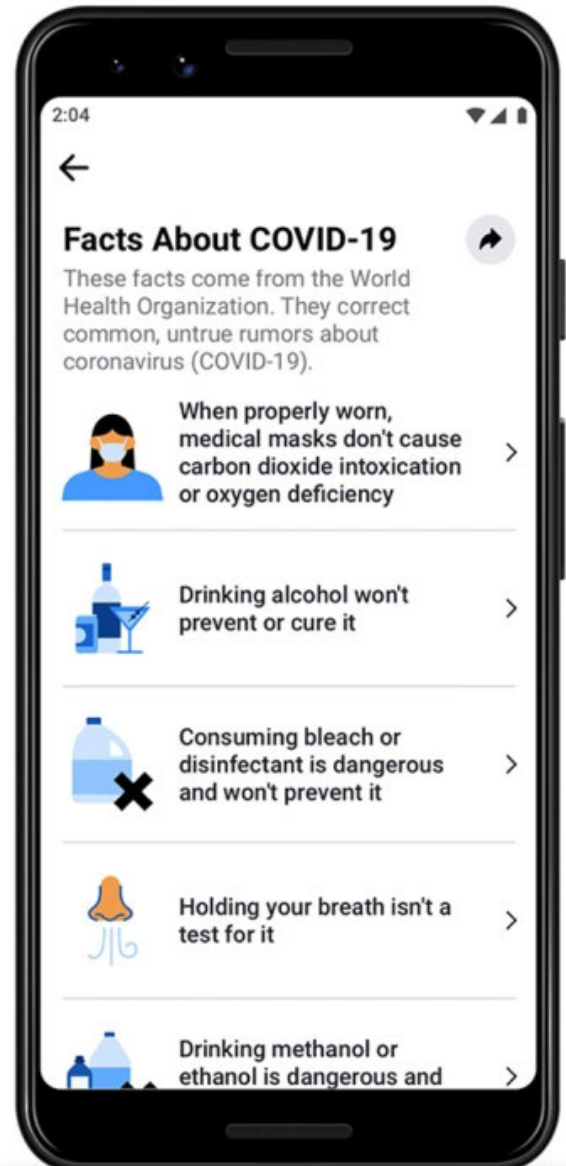
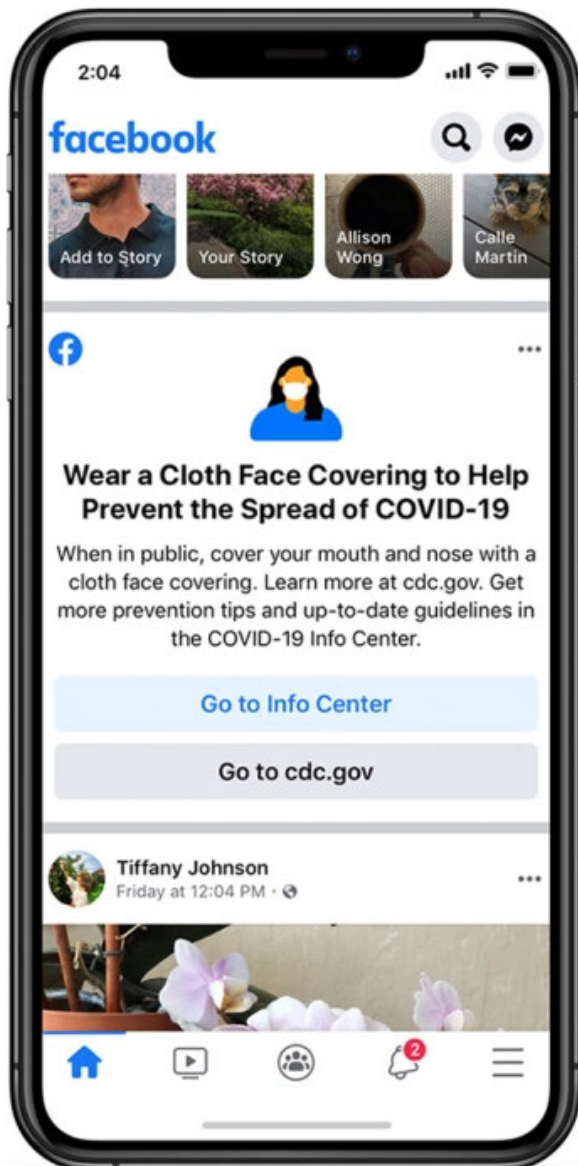
Update on July 15, 2020 at 10:00AM PT:

We continue working to keep people safe and informed about COVID-19. We have connected over 2 billion people to resources from health authorities through our [COVID-19 Information Center](#) and pop-ups on Facebook and Instagram with over 600

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 299 of 672 PageID #: 20352
million people clicking through to learn more. Since January, people have raised over \$100 million for COVID-19 related fundraisers on Facebook and Instagram. Over half of those donations were under \$25.

Facts About COVID-19

To further limit the spread of misinformation, this week we are launching a dedicated section of the COVID-19 Information Center called Facts about COVID-19. It will debunk common myths that have been identified by the World Health Organization such as drinking bleach will prevent the coronavirus or that taking hydroxychloroquine can prevent COVID-19. This is the latest step in our ongoing work to fight misinformation about the pandemic.

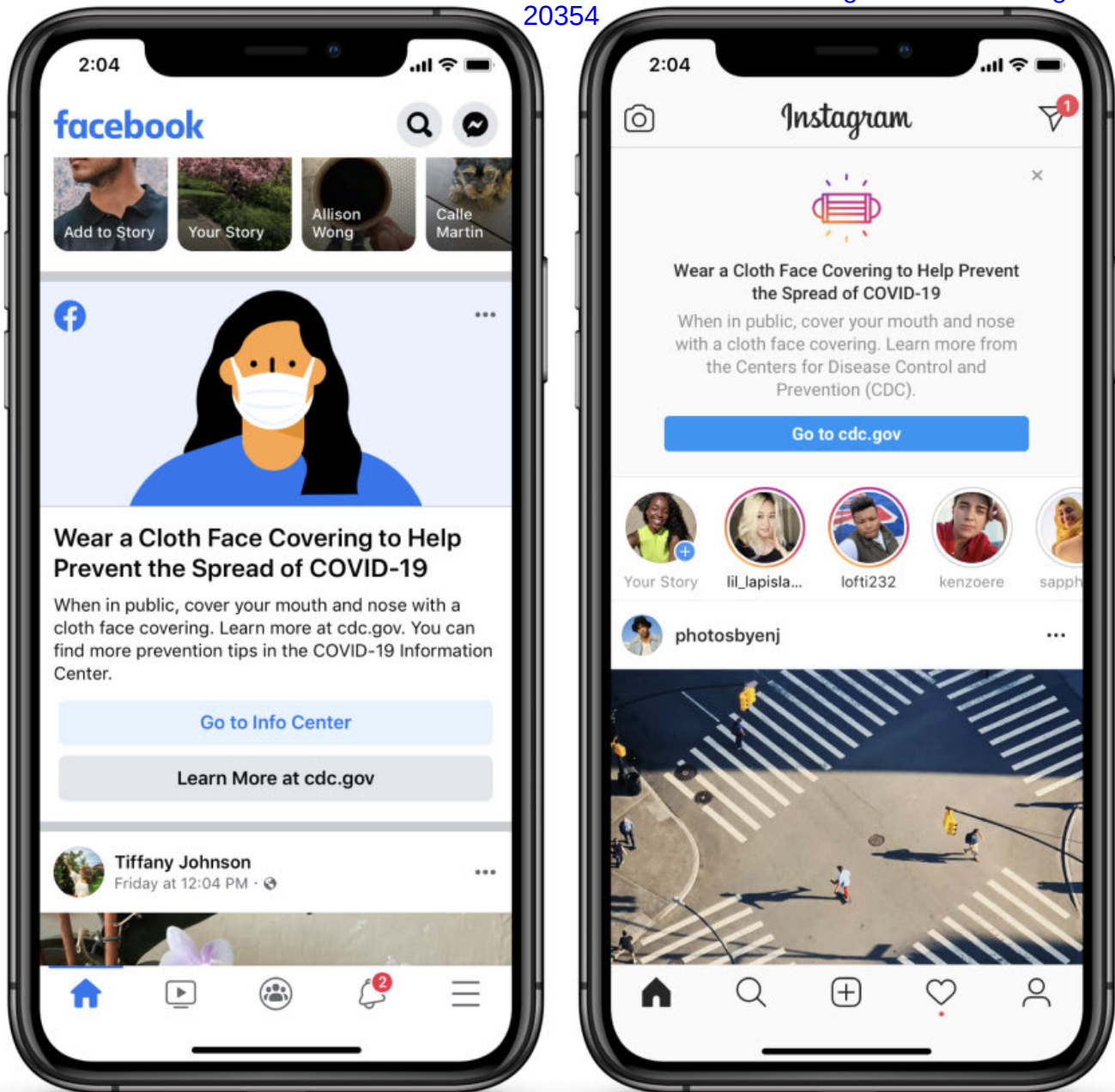


Global Reminders to Wear Face Coverings

With the rise in COVID-19 cases in the US and in many other parts of the world, we are expanding our alerts reminding people to wear face coverings internationally as recommended by health authorities. These alerts have been running at the top of Facebook and Instagram in the US since early July. Starting this week, we will expand them to more countries globally.

Update on July 2, 2020 at 9:00AM PT:

With the rise in COVID-19 cases in the US, we're putting an alert at the top of Facebook and Instagram to remind everyone to wear face coverings and find more prevention tips from the CDC in our COVID-19 Information Center.



Update on June 24, 2020 at 5:00AM PT:

Launching Summer of Support

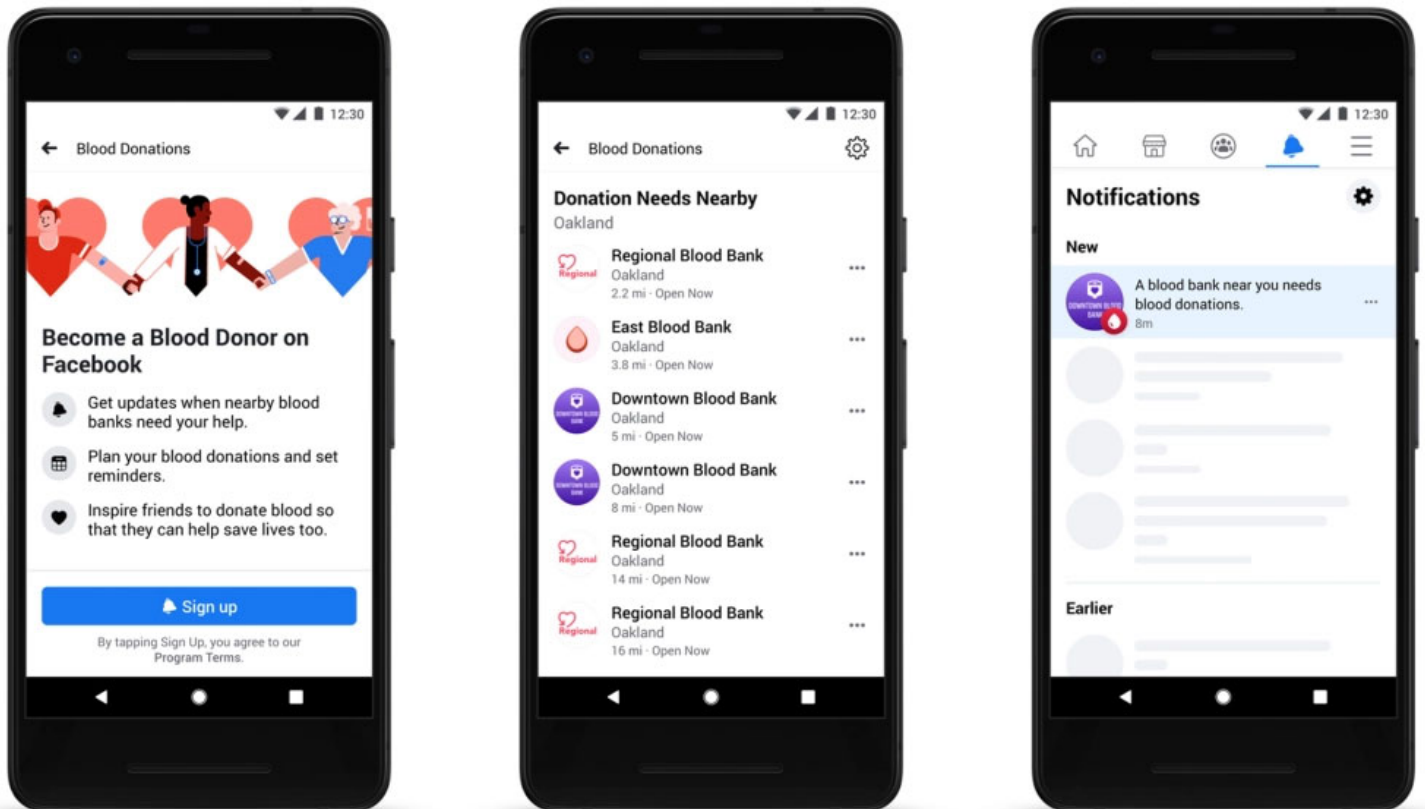
Over the past few months, many businesses have changed the way they operate, and many more are looking for ways to pivot and move forward. Today we're kicking off our Boost with Facebook Summer of Support program to help millions of people get training in the digital skills they need to succeed. Over the next six weeks, we'll offer free online training, live sessions and conversations on topics such as reimagining

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 302 of 672 PageID #: 20355
customer support, transitioning from brick and mortar to digital, and more. You can learn more about Summer of Support and other ways we're supporting businesses [here](#).

Update on June 11, 2020 at 12:01AM PT:

Expanding Our Blood Donations Feature

COVID-19 has led to blood shortages around the world due to shelter in place orders limiting the ability for people to donate. To help, we're expanding our Facebook [Blood Donations feature](#) to connect more people to their local blood banks, so they know when there is a shortage and where it is safe to donate. The Blood Donations feature is now available in South Africa, Senegal, Kenya, Burkina Faso, Côte d'Ivoire and Egypt as well as the US, India, Brazil, Pakistan and Bangladesh. We're also working with partners in India and Brazil to connect people with more local blood banks and hospitals through the Blood Donations feature. And in the US, we're excited to announce a new partnership with [AABB](#) to connect people to hospital blood banks.



Allowing the Promotion of Non-Medical Masks on Facebook and Instagram

Since the World Health Organization declared COVID-19 a global pandemic, governments and authorities around the world have evolved their guidance on the need to wear masks. In March, we temporarily banned ads and commerce listings for masks on our apps to help protect against scams, misleading medical claims, medical supply shortages, inflated prices and hoarding. Since then, we've continued to monitor trends and activity around COVID-19 to better understand how people are using our platform and advertising tools during the pandemic.

Many health authorities now advise wearing non-medical masks – and in some places masks are required for activities like taking public transportation or visiting a store – and we've seen people and businesses of all sizes working to fill this need. So we're scaling back this temporary ban to allow people to promote and trade non-medical masks, including those that are homemade or handmade, in organic posts, ads and commerce listings on Facebook and Instagram. We will still maintain a temporary ban on selling medical masks, such as surgical or N95 masks, to prevent people from exploiting the pandemic for financial gain. You can learn more about how we define non-medical masks and advertiser restrictions for these ads here.

Update on June 3, 2020 at 12:01AM PT:

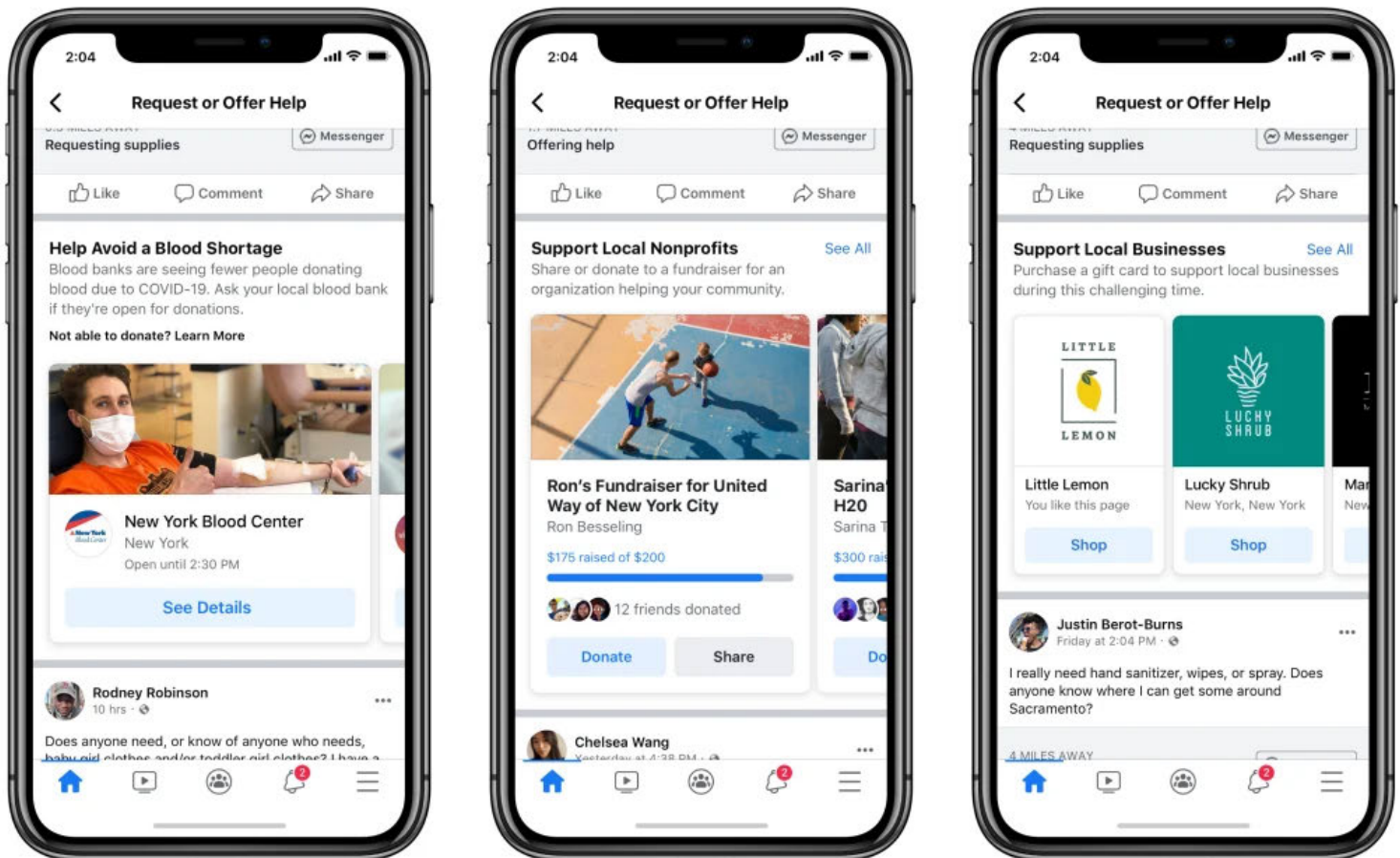
Releasing New Data for Good Tools

Today we're releasing new visualizations and datasets publicly to help researchers, NGOs and others combat the COVID-19 pandemic. You can learn more about these and our other Data for Good tools here.

Update on May 4, 2020 at 9:38AM PT:

Tomorrow on #GivingTuesdayNow we're expanding Community Help to make it easier for people to support local businesses and nonprofits. Starting tomorrow, people will be able to find gift cards and vouchers to support local businesses, donate to local

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 304 of 672 PageID #: 20357
nonprofit fundraisers, sign up to become a blood donor and find local job opportunities — all in Community Help.



Update on April 22, 2020 at 6:30AM PT:

Partnering with ITDRC and NetHope to Address the Digital Divide

The coronavirus pandemic has underscored the importance of internet connectivity. While many people have shifted their lives online, there are still more than 3.5 billion people, including more than 18 million Americans, who lack reliable internet access. To help, we're partnering with the Information Technology Disaster Resource Center (ITDRC) and NetHope to provide internet connectivity to communities most impacted by COVID-19. The goal of these partnerships is to better understand the unique barriers these communities face in getting online and create the programs and infrastructure needed to increase the availability and affordability of high-quality internet access.

- We're providing a \$2 million grant to support ITDRC's projectConnect initiative which will help rural and underserved communities in the US gain access to the internet. We're also

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 305 of 672 PageID #: 20358
sharing insights from Facebook Disease Prevention Maps to help ITDRC better understand options for internet coverage in specific regions and more quickly determine the type of support needed to address connectivity challenges.

- We're providing a \$260,000 grant to support NetHope's COVID-19 response. In addition, through sharing our Disease Prevention Maps, we'll help NetHope identify the world's most vulnerable and affected communities, including migrants and refugees, in order to provide them with protective health equipment and internet connectivity kits.

Update on April 21, 2020 at 3:30PM PT:

Update on Content Review Work

Throughout the COVID-19 crisis, we've worked to keep both our workforce and the people who use our platforms safe. Last month we announced that we would temporarily send our content reviewers home. Since then we've shared updates on changes we've made to keep our platform safe during this time, including increasing the use of automation, carefully prioritizing user reports, and temporarily altering our appeals process.

We've also asked some of our full-time employees to review content related to real-world harm like child safety and suicide and self-injury. It's become clear in recent weeks that our offices are unlikely to return to business as usual in the near future. Some of our full-time employees will continue to review sensitive content, but as Mark referenced last week we will begin working with our partners to bring a small number of content reviewers back to offices to support these efforts in the coming weeks.

Returning to the office will be voluntary. We'll also work with our partners to put protections in place to keep content reviewers safe. These will include: greatly reducing building capacity in these offices to ensure government guidelines on physical distancing can be observed, implementing strict cleaning protocols and providing personal protective equipment like masks and gloves as well as temperature checks at the beginning of every shift.

As the situation evolves, we'll continue to share changes we make to keep both our community and the people who review content on our platforms safe.

Facebook Joins Open COVID Patent Pledge

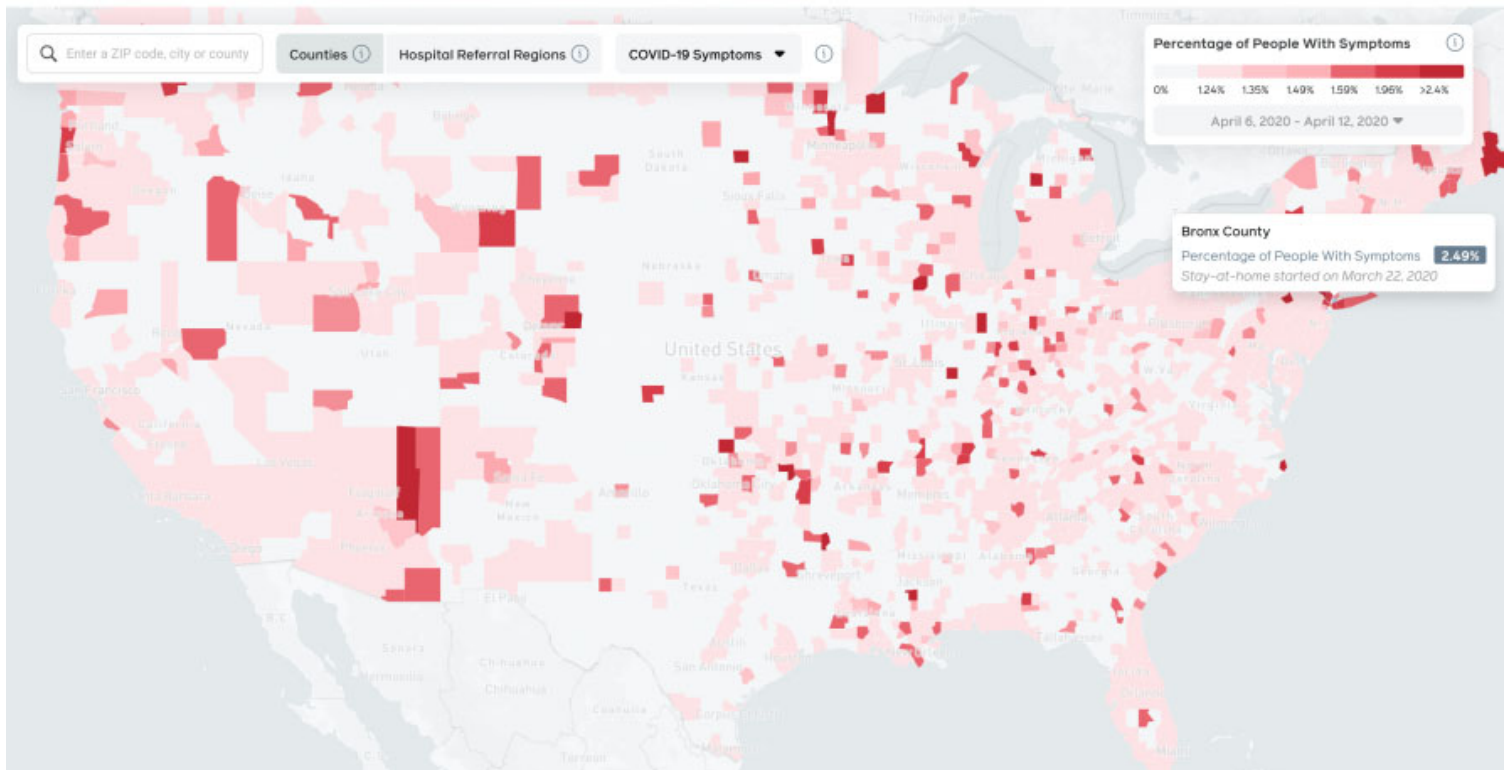
Today Facebook joined Amazon, Hewlett Packard, IBM, and Microsoft in signing the Open COVID Patent Pledge to help make patents freely available in the fight against COVID-19. The pledge allows people to use our patents to advance innovation that may help in ending the COVID-19 pandemic and minimizing the impact of the disease — without any uncertainty around intellectual property rights or fear of litigation.

Update on April 20, 2020 at 3:15AM PT:

Sharing COVID-19 Symptom Maps and Expanding Survey Globally to Help Predict Disease Spread

Today Carnegie Mellon University (CMU) Delphi Research Center made public the initial results of their US symptom survey we promoted on Facebook. Using aggregate data from Carnegie Mellon, Facebook produced its first report and new interactive maps, which we plan to update daily through this outbreak. Mark Zuckerberg wrote in the Washington Post about how surveys like this can be an important tool in fighting COVID-19 and announced that we're working with faculty from the University of Maryland to expand the program globally.

Facebook & Carnegie Mellon University COVID-19 Symptom Map



Update on April 16, 2020 at 10:55AM PT:

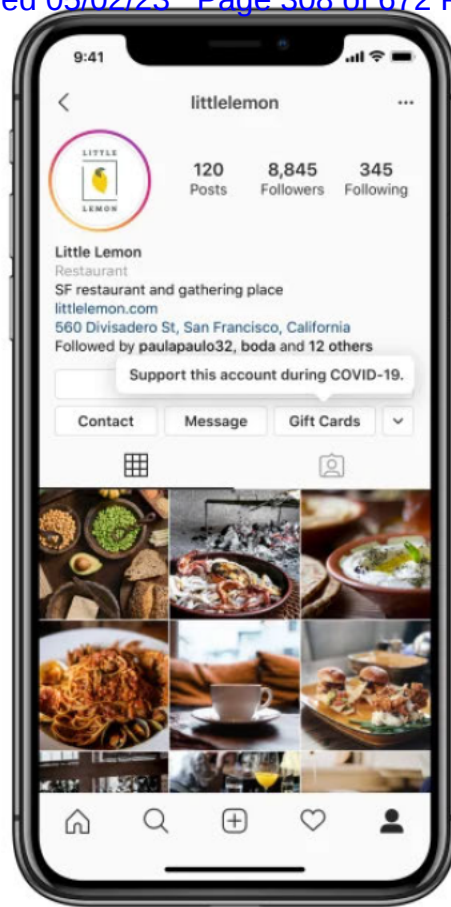
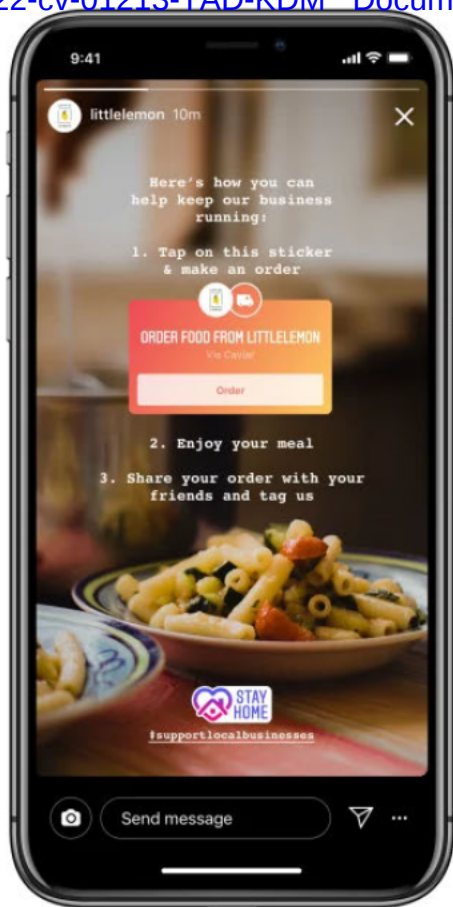
Limiting the Spread of COVID-19 Misinformation

Today we shared some additional steps we're taking to combat COVID-19 related misinformation and make sure people have the accurate information they need to stay safe.

Update on April 15, 2020 at 8:08AM PT:

Making It Easier to Support Businesses on Instagram

We're making it easier for people to support the businesses they love through gift cards, online food orders and fundraisers all on Instagram. [Learn more.](#)



Update on April 14, 2020 at 2:05PM PT:

Getting Expert Insights on How We Can Safely Re-Open Society

Mark Zuckerberg and Priscilla Chan are live with Dr. Tom Frieden, the former director of the CDC and founder of Resolve to Save Lives. They'll discuss how we can contain the spread of COVID-19 and how we should approach reopening society.



Live with Priscilla and Dr. Tom Frieden, th...

Mark Zuckerberg was live

Share

Facebook Watch

Helping the WHO Share Timely Information on Messenger

Today the World Health Organization (WHO) launched an interactive experience on Messenger to provide accurate and timely information about the coronavirus outbreak. People will now be able to message the WHO with questions about COVID-19 and get quick answers for free. The WHO created this Messenger experience with support from Sprinklr as part of the program we recently announced to pair developer partners with health organizations to help them connect with people and deliver critical information during the COVID-19 outbreak. Learn more.

Update on April 9, 2020 at 2:15PM PT:

Connecting People to Well-Being Tips and Resources

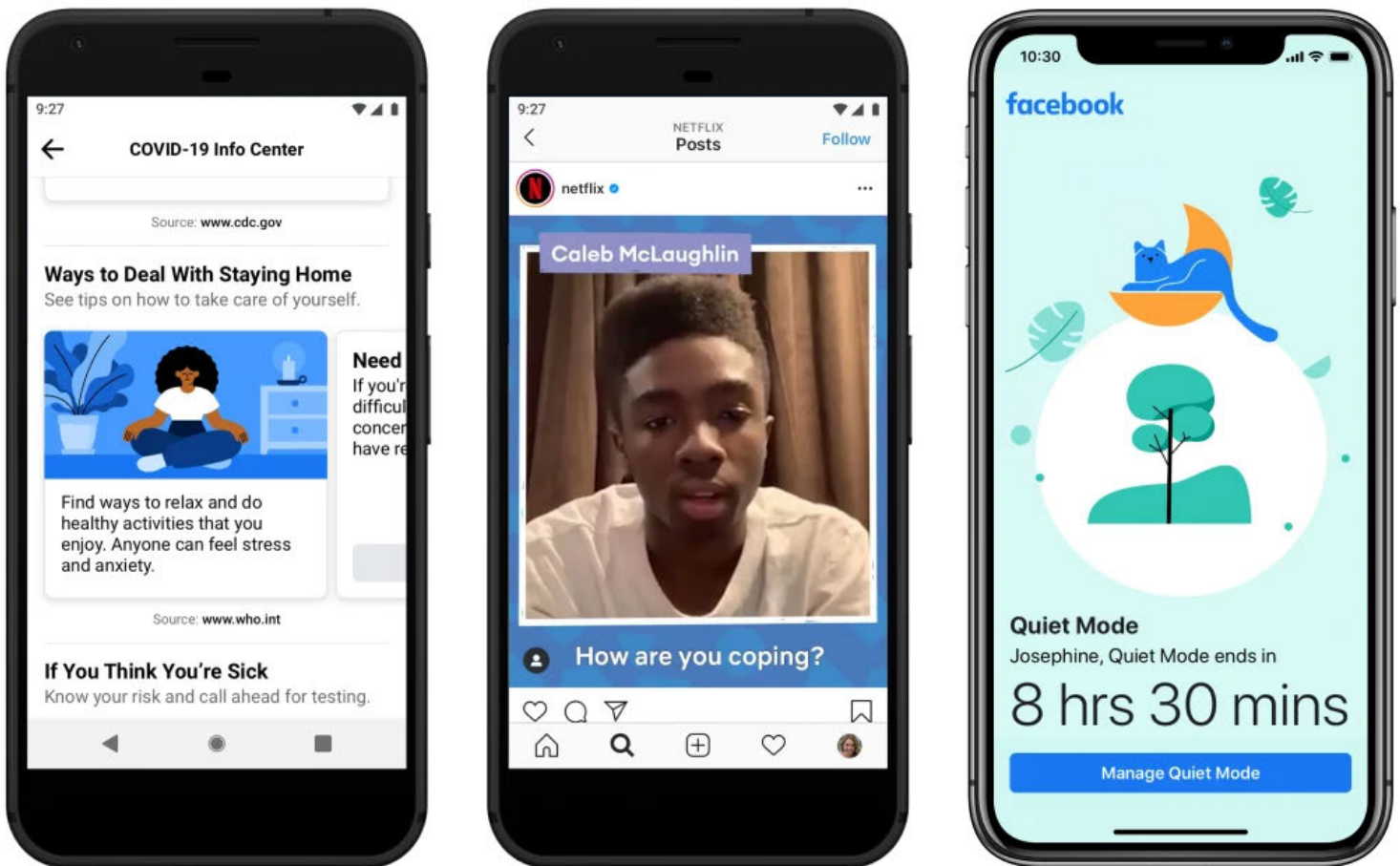
The COVID-19 pandemic has forced people around the world to adjust to new routines, cope with loneliness, job loss, grief and more. And it's tough for all of us in different ways, not just physically but mentally. To help, we're sharing tips from experts to stay well, supporting the work of mental health organizations, and giving you tools to manage your time on Facebook.

- **Tips and Resources:** We're sharing tips from the World Health Organization (WHO) on how people can take care of themselves, stay active, relieve stress, and establish new goals and routines while staying home. We'll also connect people to their local crisis hotline, so people can call or text to get help when they need it. These tips and resources will be available in the Coronavirus Information Center on Facebook starting today, and we'll also share similar well-being tips on @Instagram from the National Alliance on Mental Illness (NAMI).
- **Mental Health Live Series:** We're encouraging people to tune in to an Instagram Live series from @Netflix called "Wanna Talk About It?" Stars will pair up with experts from organizations like the American Foundation for Suicide Prevention, NAMI, Crisis Text Line, The Trevor Project, Mental Health America and more to discuss how they're coping during this time as well as ways to handle anxiety, stress and feelings of isolation while social distancing. We're also working on an Instagram Live series with NAMI to encourage conversations about mental health and promote activities to help people stay well.
- **Supporting Crisis Helplines:** We're donating \$2 million to support organizations like Vibrant Emotional Health that operates the National Suicide Prevention Lifeline in the US, Kids Help

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 310 of 672 PageID #: 20365

Phone in Canada, ICALL Psychosocial Helpline in India, Samaritans in the UK, Centro de Valorização da Vida in Brazil and more. These organizations offer critical support for people struggling with loneliness, anxiety and other mental health issues and we want to help them increase capacity quickly during this time.

- **Tools to Manage Your Time:** As we all adjust to new routines and staying home, setting boundaries for how you spend your time online can be helpful. Whether it's to help you focus on your family and friends, sleep without distraction or manage how you spend your time at home, we have tools that can help you find the right balance for how you use Facebook. We added Quiet Mode, which mutes most push notifications, and if you try to open Facebook while in Quiet Mode, you'll be reminded that you set this time aside to limit your time in the app. We also added shortcuts to Notification Settings and News Feed Preferences, so you can make the most of your time on Facebook by controlling the type of posts you see in your News Feed as well as the updates you receive.



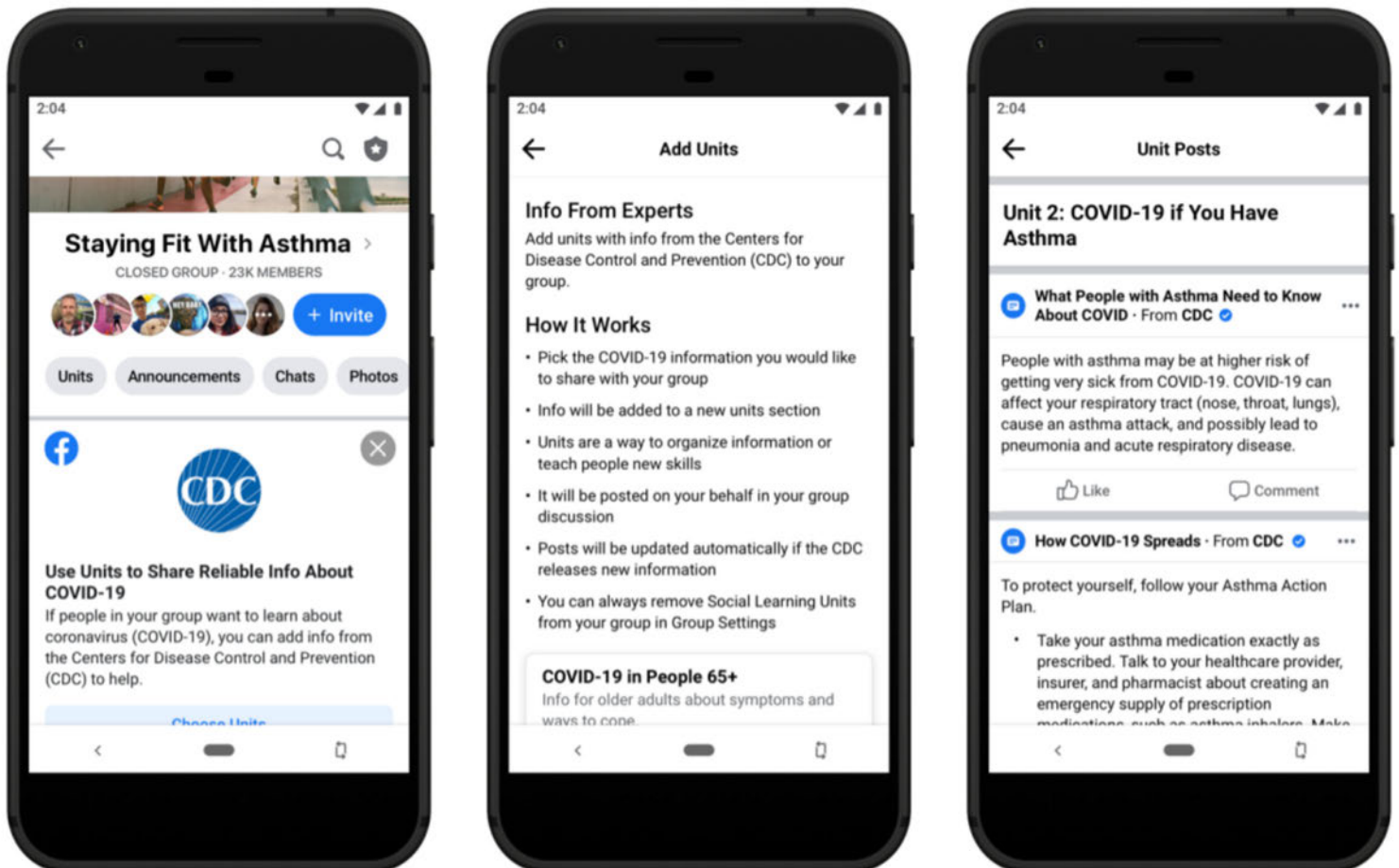
Update on April 7, 2020 at 1:00PM PT:

Helping People Get Reliable Information In Groups and Local Alerts

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 311 of 672 PageID #: 26384

As people are turning to Groups to connect with communities they care about and get support during this time, we want to make it easy to find and share reliable information in groups. Here are a few things we're doing:

- We show members of COVID-19 related groups an educational pop-up directing them to credible information from health organizations. This is similar to the messages we show in News Feed and in Search when you look for COVID-19 related content.
- We prompt group admins to share Live broadcasts about COVID-19 from health authorities like the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO) as well as official state and country health departments.
- We partnered with the CDC to develop a curriculum in our learning units tool that group admins can share with members to help them learn how to stay safe during the COVID-19 outbreak and prevent the spread of the disease.

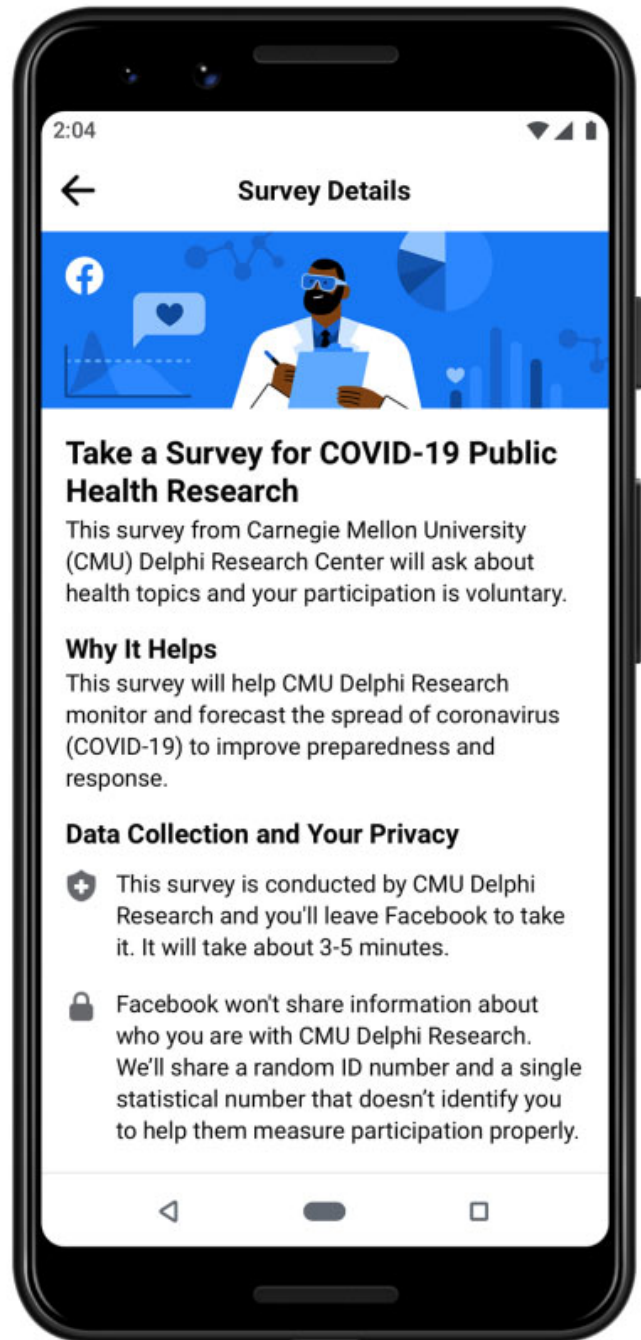
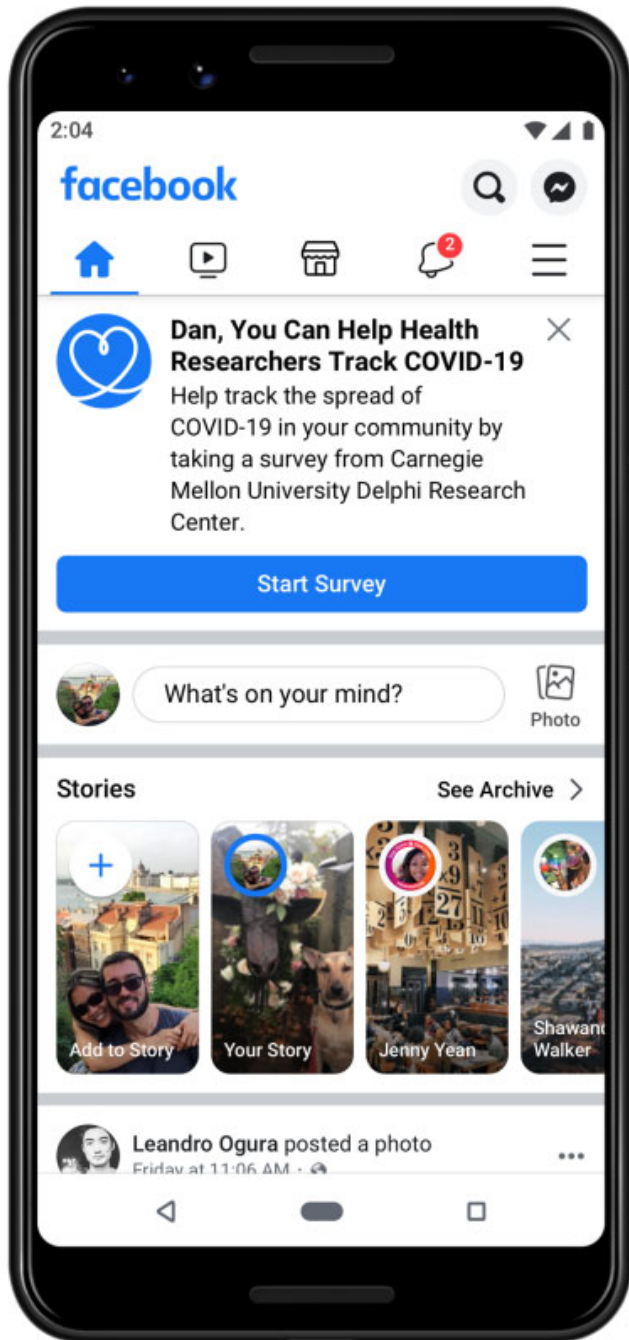


In addition, we more than doubled the number of state and local governments and health agencies onboarded to Facebook local alerts, so we now have more than 2,000 partners using the tool to communicate timely information to their communities.

New Tools to Help Health Researchers Track and Combat COVID-19

Today we're announcing new Data for Good tools to support health researchers and nonprofits:

- Three new types of Disease Prevention Maps to help inform disease forecasting efforts and protective measures, using aggregated data to protect people's privacy
- A prompt on Facebook encouraging people in the US to participate in a voluntary survey from Carnegie Mellon University Delphi Research Center designed to help health researchers identify COVID-19 hotspots earlier



Update on April 2, 2020 at 4:25PM PT:

Helping Small Businesses

Today we're sharing an update on our efforts to help small businesses get through this challenging time. These include:

- Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 314 of 672 PageID #: 20367
- **Updates to Our \$100 Million Small Business Grants Program:** We will give \$40 million in the US, which will provide grants to 10,000 businesses. We're working with Ureeka, a third-party partner to distribute these grants starting in the 34 locations where our employees live and work. Businesses can go to facebook.com/grantsforbusiness to see eligibility criteria, and applications will open in the US next week.
 - **Gift Cards:** We're making it easier for people to support their favorite local businesses with digital gift cards on Facebook, which are beginning to roll out today in the US. People will see the option to support local businesses with digital gift cards in their News Feed. Businesses interested in promoting their gift cards can [learn how to sign up](#) with one of our partners. We're also working on offering gift cards on Instagram.
 - **Fundraising:** Starting today, business owners can [create a personal fundraiser on Facebook](#) for their business and ask customers for support during this critical time.
 - **Temporary Service Changes:** To help businesses inform their customers about temporary changes, like different operating hours or delivery options during this time, we're making it possible for businesses to announce [temporary service changes](#) on their Facebook Page and in searches on Facebook.



Sheryl Sandberg
about 3 years ago



The COVID-19 pandemic has hit small businesses everywhere. Suddenly and, through no fault of their own, many simply can't do business, and for others it has become much, much harder because customers are doing the right thing and staying at home.

Facebook is committed to helping them. That's why we recently announced our \$100 million global small business grant program and why we are providing more details today about how businesses can apply, when we will start accepting app...

[See more](#)



FACEBOOK.COM

Our Continued Support for Businesses Through the Coronavirus ...

Facebook is continuing to support small businesses through the COVID-19 pand...

640

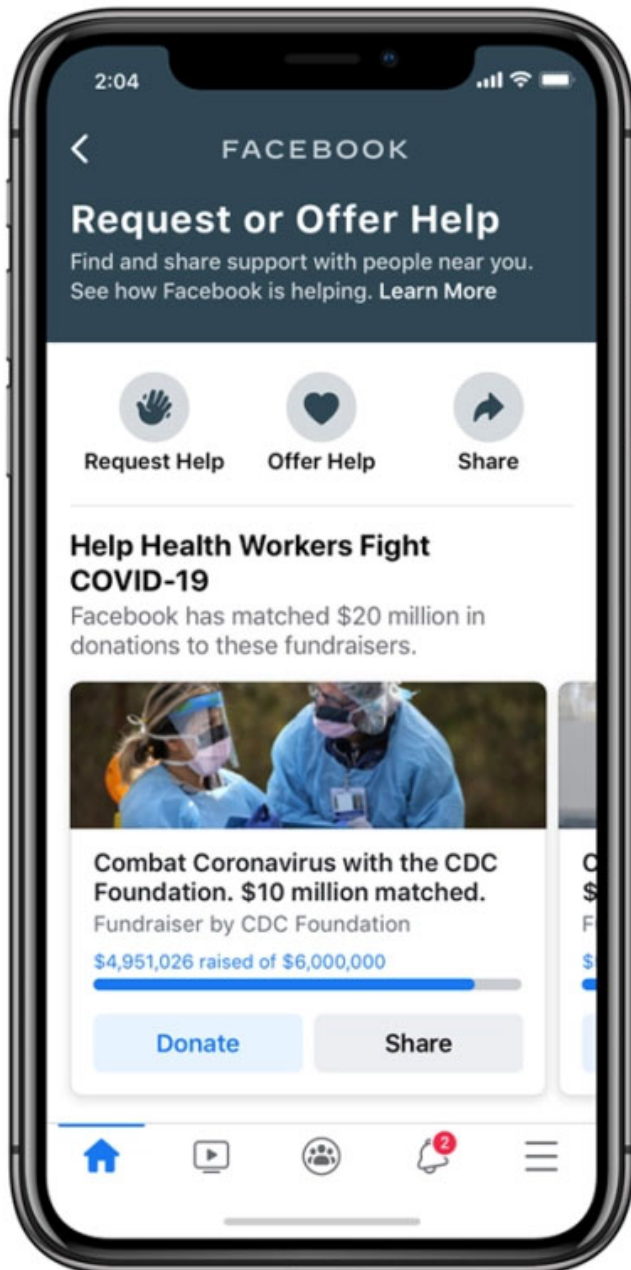
90

192

Update on March 31, 2020 at 12:15PM PT:

Making It Easier for People to Request or Offer Help in Their Communities

Today we're announcing Community Help, a place for people to request or offer help to neighbors, such as volunteering to deliver groceries or donating to a local food pantry or fundraiser. You can access Community Help in the COVID-19 Information Center on Facebook or by visiting facebook.com/covidsupport. We're starting to roll it out in the US, the UK, France, Australia and Canada in the next few days, and we're working to bring it to more countries in the coming weeks.





Mark Zuckerberg

Share

Facebook Watch

We made a short film "Never Lost" to honor the solidarity and resilience of so many people coming together during this time. Thank you to everyone doing your part. If you need help or can offer it, please visit facebook.com/covidsupport

39K

3.8K

10K

Update on March 30, 2020 at 1:40PM PT:

Donating \$25 Million to Support Healthcare Workers

Mark Zuckerberg and Priscilla Chan are live with Governor Gavin Newsom to talk about California's response to the COVID-19 outbreak. They'll discuss the urgent need for more healthcare workers and Facebook's \$25 million donation to help support healthcare workers on the front line.



Live with Governor Newsom and Priscilla ...

Mark Zuckerberg was live

Share

Facebook Watch

Investing \$100 Million in the News Industry

The news industry is working under extraordinary conditions to keep people informed during the COVID-19 pandemic. Today we're announcing an additional \$100-million investment to support journalists — including \$25 million in emergency grant funding for local news through the Facebook Journalism Project, and an extra \$75 million in marketing to get money to publishers around the world at a time when their advertising revenue is declining.

This investment is in addition to the support we've already pledged to the news industry in response to COVID-19: \$1 million in grants for local news, \$1 million in grants for fact-checking organizations, and a \$1-million donation to the International Fact-Checking Network.

Update on March 26, 2020 at 1:00PM PT:

Launching the Messenger Coronavirus Community Hub

Today, we're launching the Messenger Coronavirus Community Hub with tips and resources to keep people connected to their friends, family, colleagues and community, and prevent the spread of misinformation. It also includes advice on how to recognize and avoid scams and misinformation online. Read more about how you can use Messenger to stay connected and informed during this time.

Update on March 26, 2020 at 9:00AM PT:

Helping Young People Safely Navigate the Internet

Today we're launching our digital literacy program, Get Digital, to provide lessons and resources to help young people develop the competencies and skills they need to more safely navigate the internet. These resources are designed to be used by educators and families both in the classroom and at home, but they've become even more important as young people spend more time on their devices while at home during the COVID-19 outbreak.

- Stay safe online and protect their personal information
- Navigate content and information, and evaluate the trustworthiness of a source
- Build positive and inclusive communities online by being kind and respecting others
- Manage their health and wellbeing by learning how to monitor emotions and develop healthy habits for when to use technology

It will also help them discover how technology can be used for civic and political engagement. And it can help them develop digital skills, such as understanding algorithms, and explore programming and more to help prepare them for future careers in technology.

We're partnering with UNESCO, the International Society for Technology in Education (ISTE), National PTA, and EVERFI to distribute our new digital literacy tools to parents and educators around the world. Lessons are drawn from the Youth and Media team at the Berkman Klein Center for Internet & Society at Harvard University, which has made them freely available worldwide under a Creative Commons license, and the Greater Good Science Center.

Update on March 26, 2020 at 7:15AM PT:

Sharing Tips for People Working Remotely

Remote work can be challenging whether you're balancing caregiving and work, trying to lead a dispersed team, or adjusting to a new routine and responsibilities. That's why we created an online resource with tips to help our global team stay connected, be productive and do their best work, wherever they're working. We're sharing it publicly today in case it's helpful to others as many adjust to working remotely during this challenging time. Check out our [remote work resources](#).

Update on March 25, 2020 at 9:57AM PT:

Combating COVID-19 Misinformation Across Our Apps

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 320 of 672 PageID #: 20373
Today we shared an overview of how we're connecting people to reliable information and taking aggressive steps to combat COVID-19 misinformation across our apps.

Update on March 24, 2020 at 1:30PM PT:

Keeping Our Apps Stable and Reliable

As more people around the world are physically distancing themselves from others, we've seen people using our apps more than ever. Today, we shared some data to give context on the load we're managing. Our apps were built to withstand spikes, but the usage growth from COVID-19 is unprecedented across the industry. We're monitoring usage patterns carefully, making our systems more efficient and adding capacity when needed, and we're doing everything we can to keep our apps stable and reliable during this time.

Update on March 24, 2020 at 6:00AM PT:

Helping People Stay Informed and Connected on Instagram

Today we announced updates to help people stay informed, safe and connected on Instagram during this challenging time. These include:

- Adding more educational resources in Instagram Search
- Adding stickers to promote accurate information
- Removing COVID-19 content and accounts from recommendations, unless posted by a credible health organization
- Rolling out the donation sticker in more countries and helping people find relevant nonprofits to support
- Creating a shared story to help those practicing social distancing connect with others, using a "Stay Home" sticker
- Launching a new way to browse Instagram with friends over video chat

Helping Government Health Organizations Use Messenger

Today we're announcing two initiatives to help government health organizations in their response to the coronavirus outbreak using Messenger.

1. We're connecting government health organizations and UN health agencies with our developer partners who will help them use Messenger most effectively to scale their response to COVID-19. Our developer partners will provide their services for free, showing these critical organizations how to use Messenger to share timely information with local communities and speed up their replies to commonly asked questions with tools like automated responses.
2. We're also starting an online hackathon and inviting developers to build messaging solutions that address issues related to the coronavirus such as social distancing and access to accurate information. Participants will receive unique access to Messenger tools and content as well as educational materials from Facebook to support their innovation. And the winners will get mentoring from Facebook engineers to help make their idea a reality.

[Read more](#) about how we're leveraging Messenger's reach, tools and technology to help people stay connected and informed during this time.

Update on March 20, 2020 at 2:45PM PT:

Launching the WHO Health Alert on WhatsApp

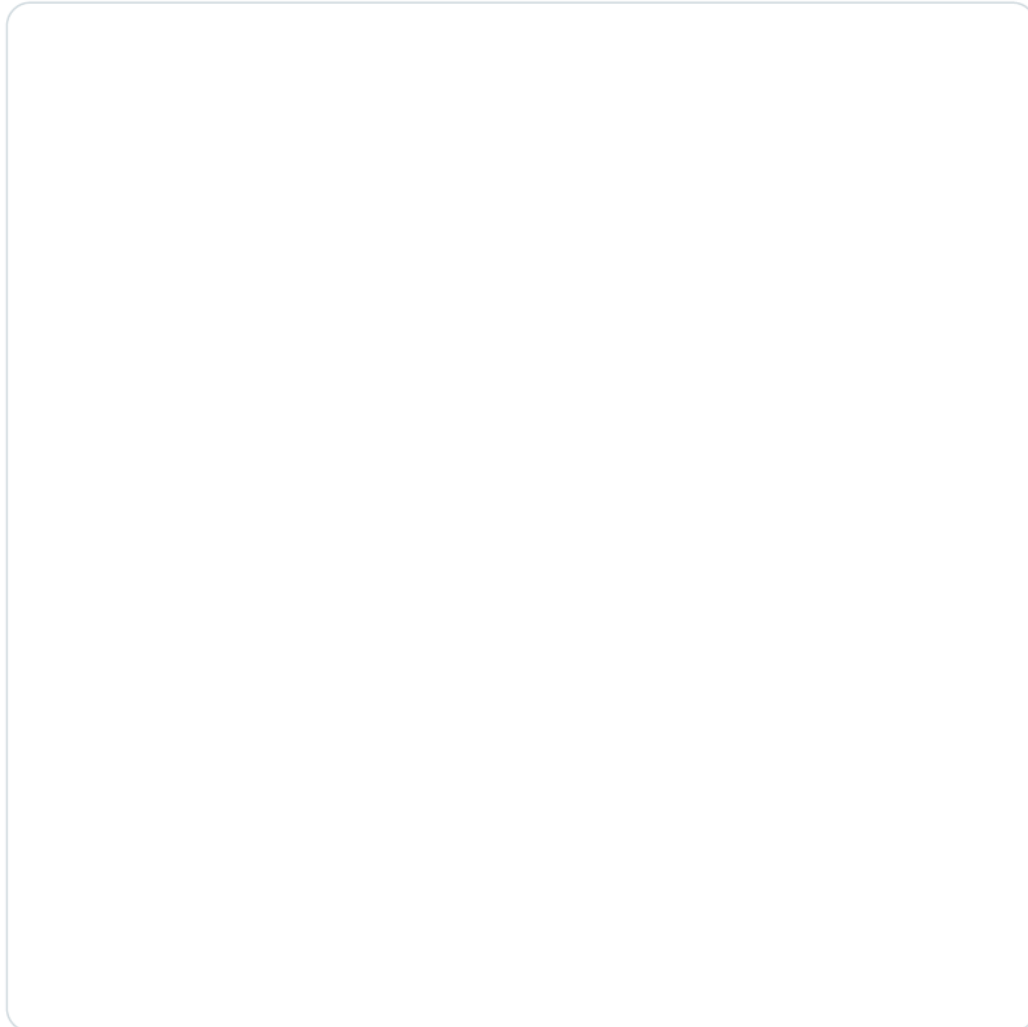
Today we launched the World Health Organization's Health Alert on WhatsApp. The [WHO Health Alert](#) is free to use and will answer common questions about COVID-19. It provides timely, reliable information about how to prevent the spread of the coronavirus as well as travel advice, coronavirus myth debunking and more. To [contact the WHO Health Alert](#), save the number +41 79 893 1892 in your phone contacts and then text the word 'Hi' in a WhatsApp message to get started. The service is initially launching in English but will be available in all six United Nations languages (English, Arabic, Chinese, French, Russian and Spanish) within the coming weeks.

WhatsApp 

@WhatsApp · [Follow](#)



It's an honor to work with [@WHO](#) to provide this simple service to get the latest information directly from the experts right on WhatsApp. Tap the link below to get started. Share these tips and de-bunked rumors with your friends and family 🙏 bit.ly/who-covid-19-w...



5:14 PM · Mar 20, 2020



 4.7K

 Reply

 Share

[Read 470 replies](#)

Update on March 19, 2020 at 7:22PM PT:

Keeping Our Platform Safe With Remote and Reduced Content Review

We recently announced that we're temporarily sending content reviewers home. We want to make sure our platform remains a safe place for people to connect during this time, but with a reduced and remote workforce, below are some ways our content review processes will be impacted.

Policy Enforcement: We will continue to enforce our policies and prioritize preventing and disrupting harm across our platform. We are conducting human rights due diligence, looking at potential risks, and putting in place contingency plans that both prioritize the safety of our content reviewers and support the integrity of our platform. As Mark Zuckerberg discussed on a press call, for example, we have shifted certain content review work to full time employees and are focusing on areas including child safety, terrorism, suicide and self-injury, and harmful content related to COVID-19.

Some contract reviewers will work from home, but with a reduced and remote workforce, we will now rely more on our automated systems to detect and remove violating content and disable accounts. As a result, we expect to make more mistakes, and reviews will take longer than normal, but we will continue to monitor how our systems are performing and make adjustments. In addition, reviewing content can be challenging, and working from home presents new obstacles in providing support to our teams, but we're working to ensure our content reviewers have the resources and help they need during this time.

User Reports: When people report content to us that they believe violates our policies, they will see a new message letting them know that we have fewer content reviewers available and will prioritize reported content that has the greatest potential to harm our community. This means some reports will not be reviewed as quickly as they used to be and we will not get to some reports at all.

Appeals: Normally when we remove content, we offer the person who posted it the option to request that we review the content again if they think we made a mistake. Now, given our reduced workforce, we'll give people the option to tell us that they disagree with our decision and we'll monitor that feedback to improve our accuracy, but we likely won't review content a second time.

We're working hard to minimize any impact on people as they use Facebook, Instagram and Messenger during this time, but we know some may feel this impact either when reporting content to us or appealing content we remove.

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 324 of 672 PageID #: 20877
We're doing everything we can to keep our global teams and the community that uses our apps safe while continuing to provide the services people and businesses rely on.

Update on March 19, 2020 at 4:12PM PT:

Getting Expert Health Tips and Information From Dr. Fauci

Mark Zuckerberg is live with Dr. Anthony Fauci, America's top infectious disease expert involved in leading our government's response to COVID-19. They'll discuss how we can all help fight the spread of the coronavirus and what governments are doing to respond to the pandemic.



Mark Zuckerberg was live

Share

Facebook Watch

Update on March 19, 2020 at 2:18PM PT:

Banning Ads for Hand Sanitizer, Disinfecting Wipes and COVID-19 Testing Kits

In addition to masks, we're now also banning ads and commerce listings for hand sanitizer, surface disinfecting wipes and COVID-19 testing kits. And if we see people selling these products in organic posts on Facebook or Instagram, we'll remove them.

Rob Leathern  · Mar 19, 2020

20378



@robleathern · [Follow](#)

In addition to masks, we're now also banning hand sanitizer, surface disinfecting wipes and COVID-19 test kits in ads and commerce listings. This is another step to help protect against inflated prices and predatory behavior we're seeing (1/2)

Rob Leathern 

@robleathern · [Follow](#)

We'll be ramping up our automated enforcement for ads and commerce next week. If we see abuse around these products in organic posts, we'll remove those, too (2/2)

4:45 PM · Mar 19, 2020



 24  Reply  Share

[Read 8 replies](#)

Update on March 18, 2020 at 6:01PM PT:

Minimizing Disruptions for Businesses and Partners on Our Platform

As we announced on Monday, we're working with our partners to send home all contract workers who perform content review, until further notice. Since this includes people who review ads and monetized content, we wanted to share more about what this means for advertisers, publishers and creators that use our tools.

For Advertisers

We use a combination of people and technology to review ads on Facebook and Instagram, and our automated systems already play a big role in that process. Now with a reduced and remote workforce, we're relying on automated technology even more. This may mean:

- Delayed review for ads and commerce listings
- An increase in ads being incorrectly disapproved
- Delayed or reduced appeals

For Content Creators and Publishers

All monetized content goes through brand safety reviews. This includes Instant Articles and videos with in-stream ads. Since our ability to review new content is now limited, we won't be able to approve all content for monetization. We're working on how to support partners at this time.

As this situation continues to evolve, we may need to make further changes to our systems. While we're working to minimize disruptions for businesses and partners, we will inevitably make mistakes. We will do our best to address any issues as quickly as we can and continue to provide updates.

Update on March 18, 2020 at 2:30PM PT:

Press Call Recap

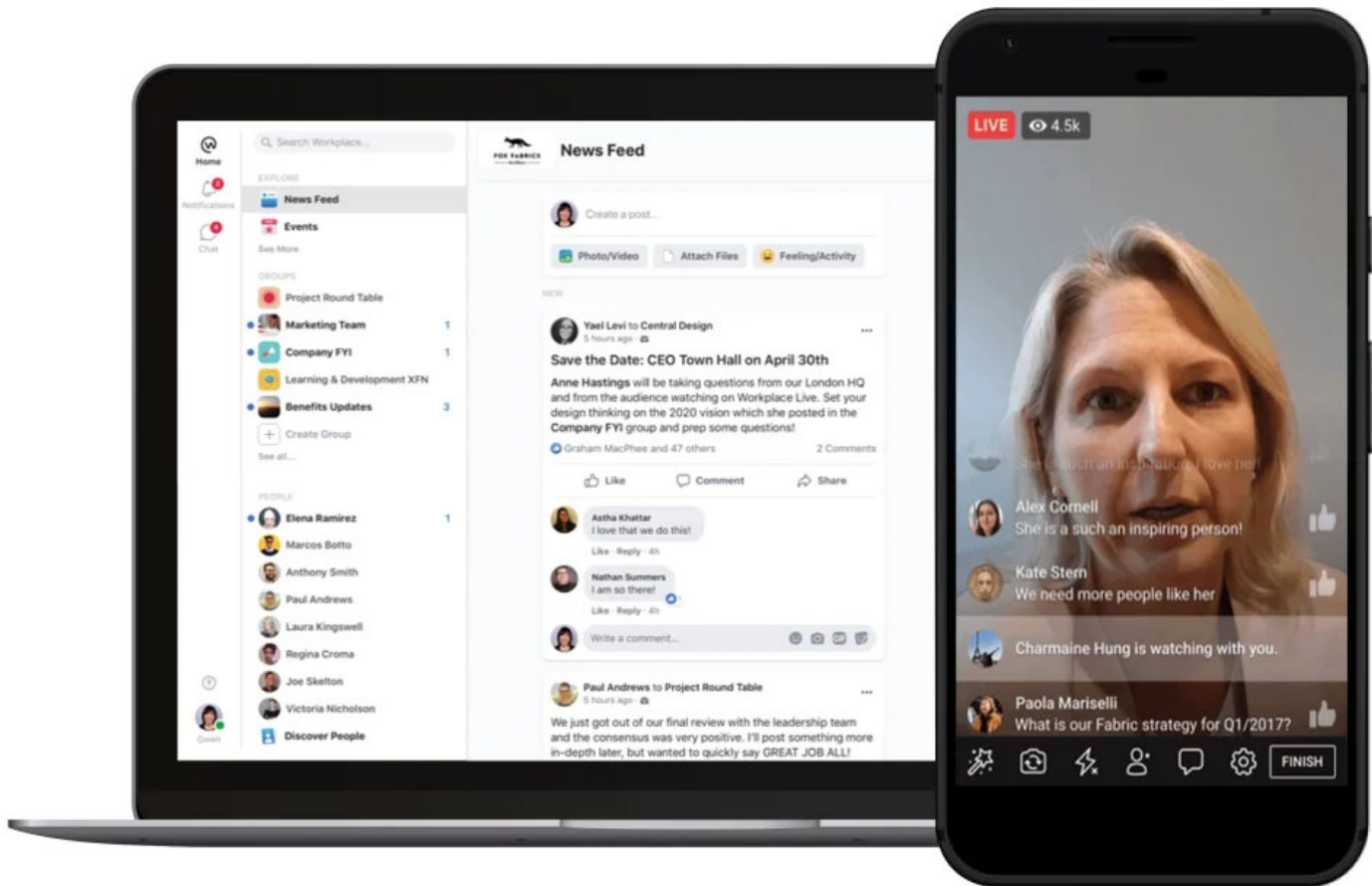
This morning on a press call, Mark Zuckerberg shared how we're supporting people and businesses affected by the coronavirus outbreak and how we're working with health authorities to make sure everyone can access accurate information. He also announced a new Coronavirus Information Center on Facebook to help people find information and tips, and he shared how we're giving governments and emergency services around the world free access to Workplace. Read the full [transcript from his press call](#).

Update on March 18, 2020 at 11:12AM PT:

Offering Workplace to Government and Emergency Organizations for Free

Starting today, we're offering Workplace Advanced to government agencies and emergency services free of charge for 12 months. These organizations play a vital role during the coronavirus outbreak, whether it's acting as first responders or coordinating public information. Workplace can help inform and connect their employees, allowing

them to share critical information in real-time and enabling leadership to reach employees via live videos, posts and more. Read more about how we're supporting emergency services and government organizations during this time.



Update on March 18, 2020 at 11:06AM PT:

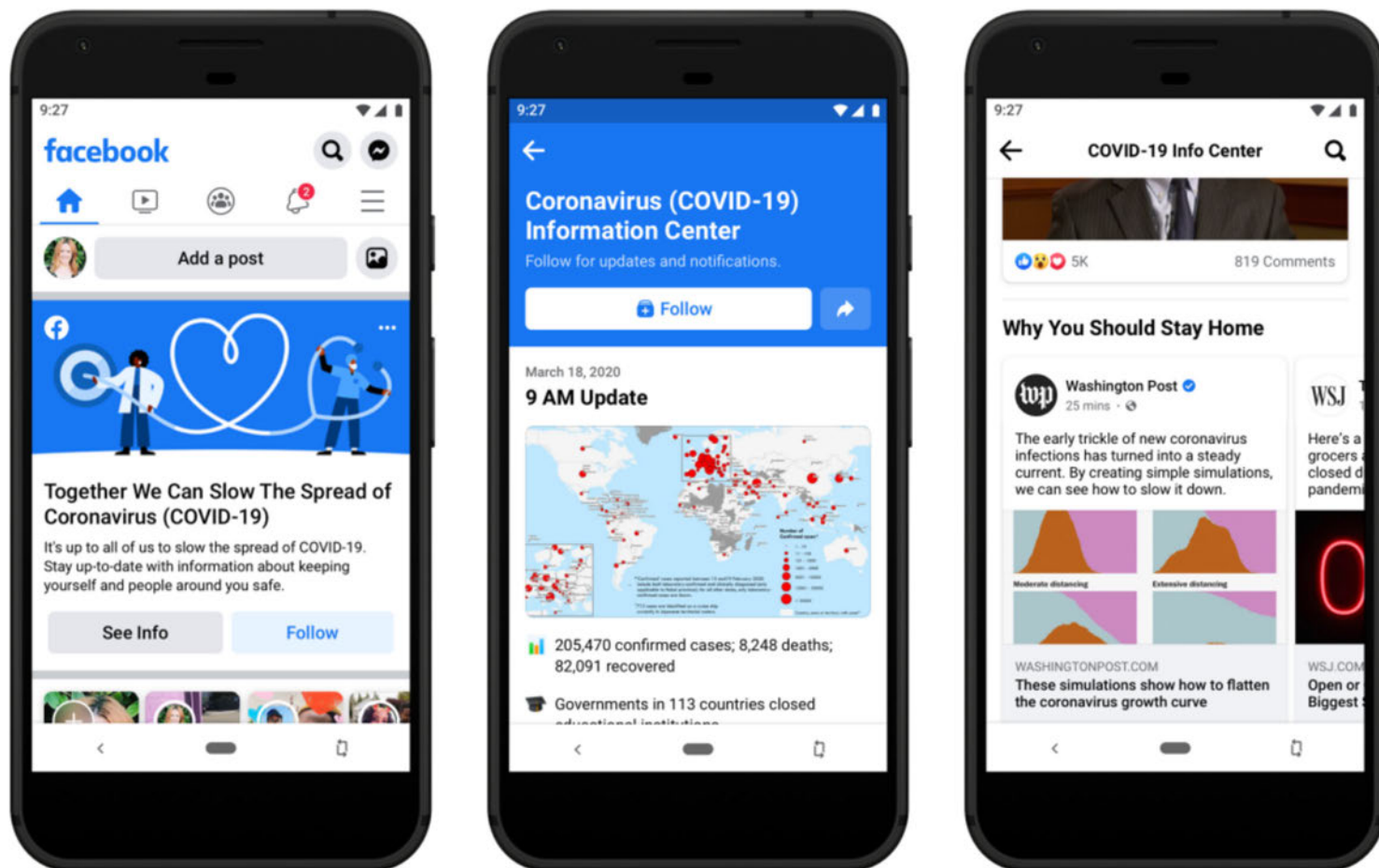
Launching the Coronavirus Information Center on Facebook

Today we're announcing the Coronavirus (COVID-19) Information Center, featured at the top of News Feed, to provide a central place for people to get the latest news and information as well as resources and tips to stay healthy and support their family and community.

It includes real-time updates from national health authorities and global organizations such as the World Health Organization, as well as helpful articles, videos and posts about social distancing and preventing the spread of COVID-19.

People can also follow the Coronavirus Information Center to receive updates from health authorities directly in their News Feed. And starting in the US, people will see features to help them connect with local groups and ask for or offer help within their community.

We're rolling out the information center in Italy, France, Germany, Spain, the UK and the US within the next 24 hours, and we'll expand it to more countries in the coming days.



Update on March 18, 2020 at 7:56AM PT:

Helping People Stay Connected Using WhatsApp

In these uncertain times, reliable communication is critical. That's why we've nearly doubled server capacity for WhatsApp and continue to see strong reliability as people place more voice and video calls around the world. In addition, today we launched an information hub with tips on how healthcare workers, educators and local businesses

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 329 of 672 PageID #: 20382
can stay connected using WhatsApp. We also donated \$1 million to the International Fact-Checking Network (IFCN) to expand the presence of local fact-checkers on WhatsApp.

Will Cathcart · Mar 18, 2020



@wcathcart · **Follow**

Today @WhatsApp has launched a hub for health workers, educators, small businesses, and others that are using WhatsApp to support one another during this extraordinary crisis. You can check it out here whatsapp.com/coronavirus

Will Cathcart

@wcathcart · **Follow**

We're grateful to @who @undp @unicef for coordinating the response to this crisis including using @WhatsApp to do so. Already several ministries of health are providing updates to citizens on WhatsApp and we will expand these services together.

10:41 AM · Mar 18, 2020



❤️ 35 💬 Reply ↗ Share

[Read 8 replies](#)

Update on March 17, 2020 at 6:15AM PT:

Supporting Fact-Checkers and Local News Organizations

To support fact-checkers in their work around COVID-19, we're partnering with The International Fact-Checking Network (IFCN) to launch a \$1 million grant program to increase their capacity during this time.

We're also supporting local news organizations as they deal with unexpected costs of covering COVID-19 and provide increased coverage during this time. To help, the Facebook Journalism Project is partnering with the Lenfest Institute for Journalism and the Local Media Association to offer a total of \$1 million in grants to local news organizations covering COVID-19 in the US and Canada.

Investing \$100 Million in Small Businesses

We're creating a \$100 million grant program to help small businesses around the world impacted by the coronavirus.



Sheryl Sandberg

about 3 years ago



As the COVID-19 outbreak escalates, our focus has been on keeping people safe and informed by making sure everyone has accurate information, supporting global health experts and stopping misinformation. Our thoughts, like everyone's, are with our loved ones and our communities and all of those impacted around the world.

In recent weeks, we have seen inspiring examples of individuals and groups helping each other. People across the globe are stepping up, rising to the enormous...

[See more](#)



FACEBOOK.COM

Facebook Small Business Grants Program

Facebook is offering \$100M in cash grants and ad credits for up to 30,000 eligibl...

1.9K

530

1.8K

Update on March 16, 2020 at 8:46PM PT:

Keeping Our People and Our Platforms Safe

To keep our people safe, we recently requested that anyone who can work from home do so in all of our offices around the world. We are also continuing to take the necessary steps to keep our platform safe.

Over the past couple of years we've substantially scaled up our investments in safety and security, including by rapidly growing content review teams and expanding our machine learning capabilities. For both our full-time employees and contract workforce there is some work that cannot be done from home due to safety, privacy and legal reasons. We have taken precautions to protect our workers by cutting down the number of people in any given office, implementing recommended work from home globally, physically spreading people out at any given office and doing additional cleaning. Given the rapidly evolving public health concerns, we are taking additional steps to protect our teams and will be working with our partners over the course of this week to send all contract workers who perform content review home, until further notice. We'll ensure that all workers are paid during this time.

We believe the investments we've made over the past three years have prepared us for this situation. With fewer people available for human review we'll continue to prioritize imminent harm and increase our reliance on proactive detection in other areas to remove violating content. We don't expect this to impact people using our platform in any noticeable way. That said, there may be some limitations to this approach and we may see some longer response times and make more mistakes as a result.

These are unprecedented times, but the safety and security of our platform will continue. We are grateful to all of our teams working hard to continue doing the essential work to keep our community safe.

Update on March 16, 2020 at 5PM PT:

Working With Industry Partners

Joint industry statement from Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter and YouTube

“We are working closely together on COVID-19 response efforts. We’re helping millions of people stay connected while also jointly combating fraud and misinformation about the virus, elevating authoritative content on our platforms, and sharing critical updates in coordination with government healthcare agencies around the world. We invite other companies to join us as we work to keep our communities healthy and safe.”

Update on March 13, 2020 at 10:10AM PT:

Matching \$20 Million in Donations to Support COVID-19 Relief Efforts

We’re matching \$20 million in donations to support COVID-19 relief efforts.



Mark Zuckerberg
about 3 years ago



A lot of people have told us they want to help fight coronavirus but aren't sure how, so we've worked with the United Nations Foundation and the World Health Organization to start a COVID-19 Solidarity Response Fund, where anyone can go to make a donation.

Facebook is matching up to \$10 million in donations, and 100% of funds will directly support the work to prevent, detect and respond to the outbreak around the world. We'll also match \$10 million for the CDC Foundation, which will launch a fundraiser in the next few weeks focused on combating the outbreak here in the US.

Thanks to everyone who is working to minimize the impact of the pandemic. More to come soon.



COVID-19 Fundraiser for WHO with up to \$10 Million Match

Fundraiser by United Nations Foundation

Your donation to this Fundraiser will go further, thanks to Facebook's matching contribution of US\$10 million. G... [Continue reading](#)

\$6,037,590 raised of \$7,000,000

Ended

147K

9.9K

20K

Update on March 13, 2020 at 9:30AM PT:

Connecting People With Credible Health Information on Instagram

We shared updates on our efforts to support the Instagram community during this time.

Instagram Comms  · Mar 13, 2020 20387



@InstagramComms · [Follow](#)

We wanted to provide some updates on our efforts to support the Instagram community at this time. The following updates will all be available from today.

Instagram Comms 

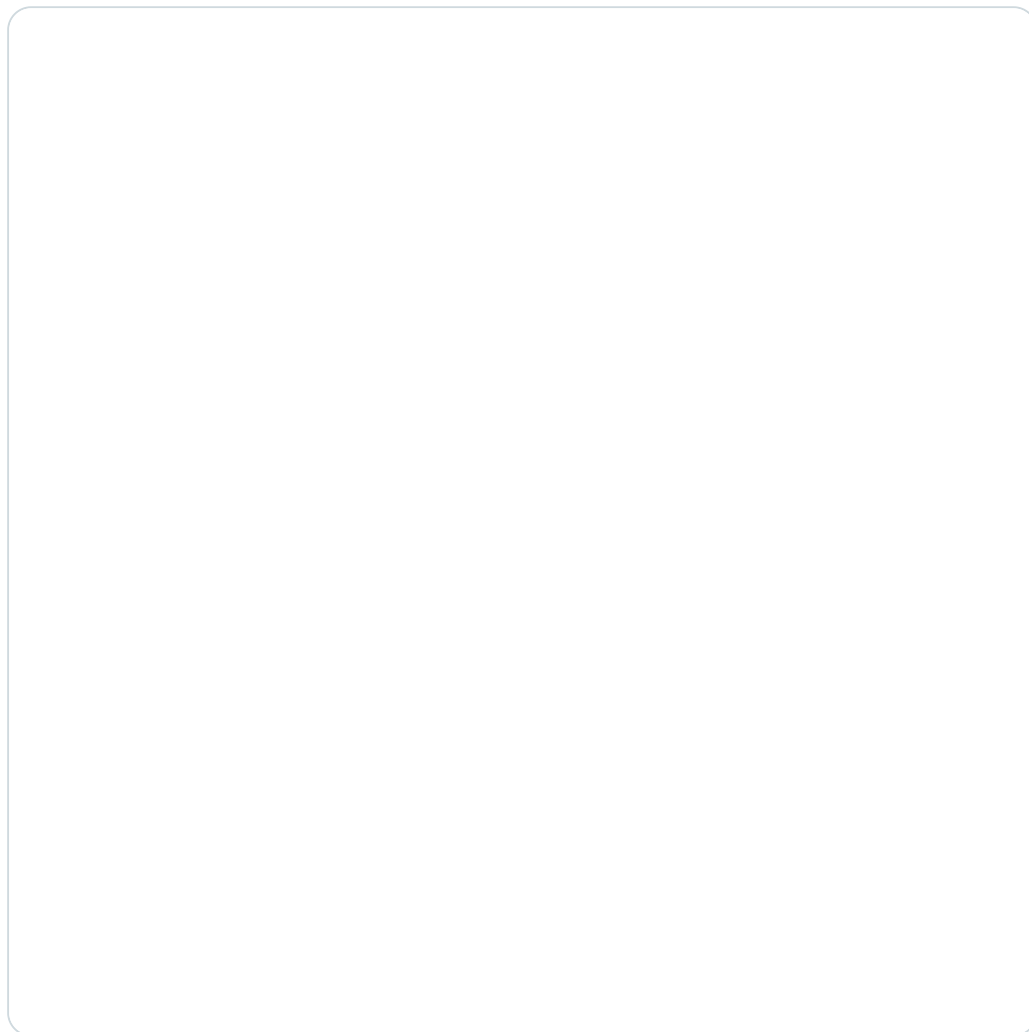
@InstagramComms

We're working to keep the Instagram community safe and informed on COVID-19. Here's an update on some of the changes we've made so far:

Instagram Comms 

@InstagramComms · [Follow](#)

To help people get relevant and up-to-date resources, we will start showing more information from [@WHO](#) and local health ministries at the top of Instagram's Feed in some countries.



12:23 PM · Mar 13, 2020



 61  Reply  Share

Instagram Comms 

· Mar 13, 2020



@InstagramComms · [Follow](#)

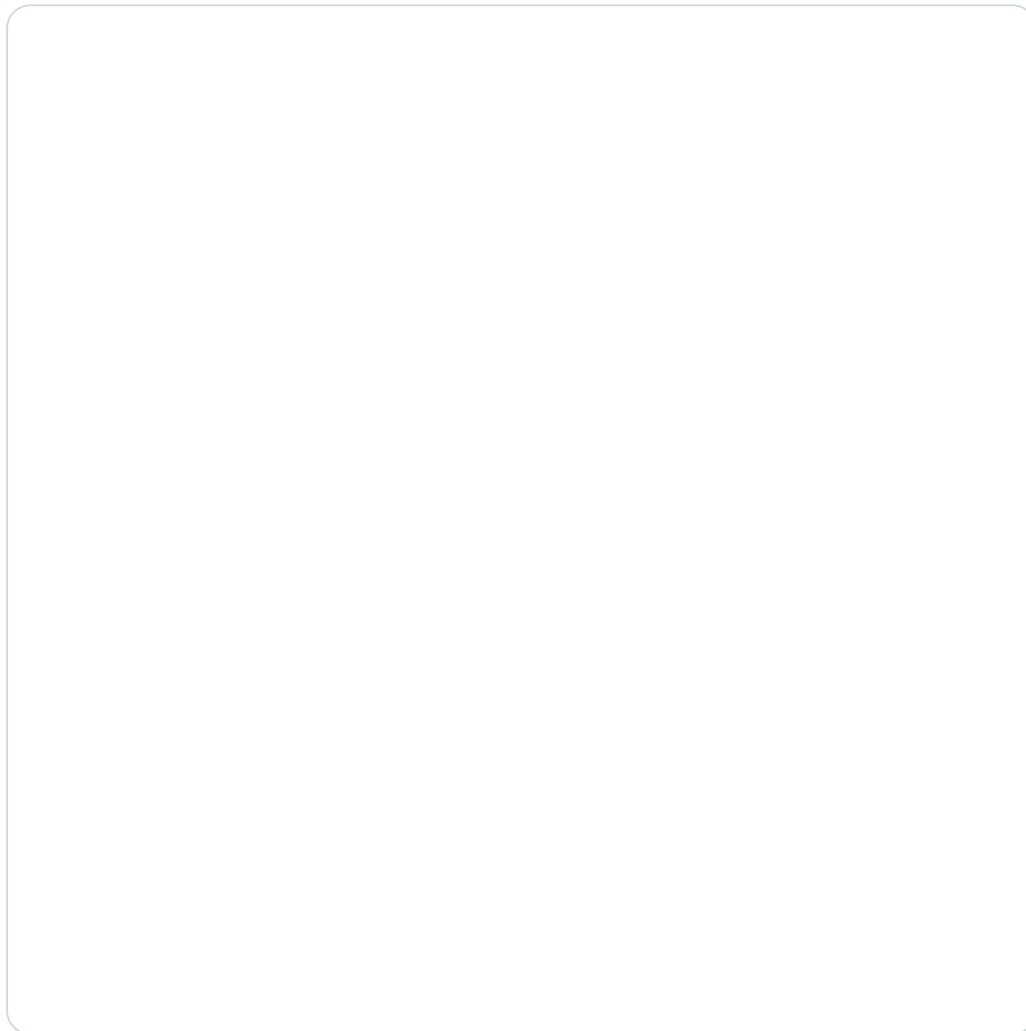
Replying to @InstagramComms

We will no longer allow people to search for COVID-19 related AR effects on Instagram, unless they were developed in partnership with a recognized health organization. This is part of our ongoing effort to better connect people with credible health information.

Instagram Comms 

@InstagramComms · [Follow](#)

To thank the health workers who have been working tirelessly to keep their communities safe, we developed a sticker for people to show their gratitude on Instagram. This will be available in the stickers gallery.



12:23 PM · Mar 13, 2020



 63  Reply  Share

[Read 16 replies](#)

Update on March 12, 2020 at 12:26PM PT:

Supporting Businesses and Community Leaders

To help people stay safe and informed during the COVID-19 outbreak, we're providing additional resources to our community. We shared a blog post on our [Community Hub](#) to provide accurate information on disease prevention and connect community leaders with tools to help them manage their community. We also created a [Business Resource Hub](#) that includes tips and trainings to help businesses navigate challenges during the COVID-19 outbreak and support their customers during this time.

Expanding Access to Facebook Local Alerts

In addition, we're helping local governments and emergency response organizations more easily communicate with their communities. As COVID-19 has spread in the US, local governments have used Facebook to share critical information with their communities about this fast evolving situation. Because of the increasing need to get timely and accurate information to local communities, we're expanding access to Facebook local alerts to even more municipal governments, state and local emergency response organizations and law enforcement agencies. State and local public health agencies will now also have the ability to push out timely, accurate information to their local communities. And we'll provide additional [training to partners](#) as they start using local alerts to share best practices for using the tool most effectively.

Eligible organizations and government agencies can [request access to the local alerts tool here](#).

Update on March 6, 2020 at 6:25PM PT:

Banning Ads and Commerce Listings for Medical Face Masks

We are temporarily banning advertisements and commerce listings, like those on Marketplace, that sell medical face masks. We'll begin to enforce this change over the next few days. We already prohibit people from making health or medical claims related

to the coronavirus in product listings on commerce surfaces, including those listings that guarantee a product will prevent someone from contracting it. We also have a dedicated channel for local governments to share listings they believe violate local laws. Our teams are monitoring the COVID-19 situation closely and will make necessary updates to our policies if we see people trying to exploit this public health emergency.



Update on March 6, 2020 at 10:52AM PT:

Removing COVID-19 Misinformation on Instagram

Today we shared updates about the changes we've made to keep the Instagram community safe and informed on COVID-19.

Instagram Comms 

· Mar 6, 2020 20391



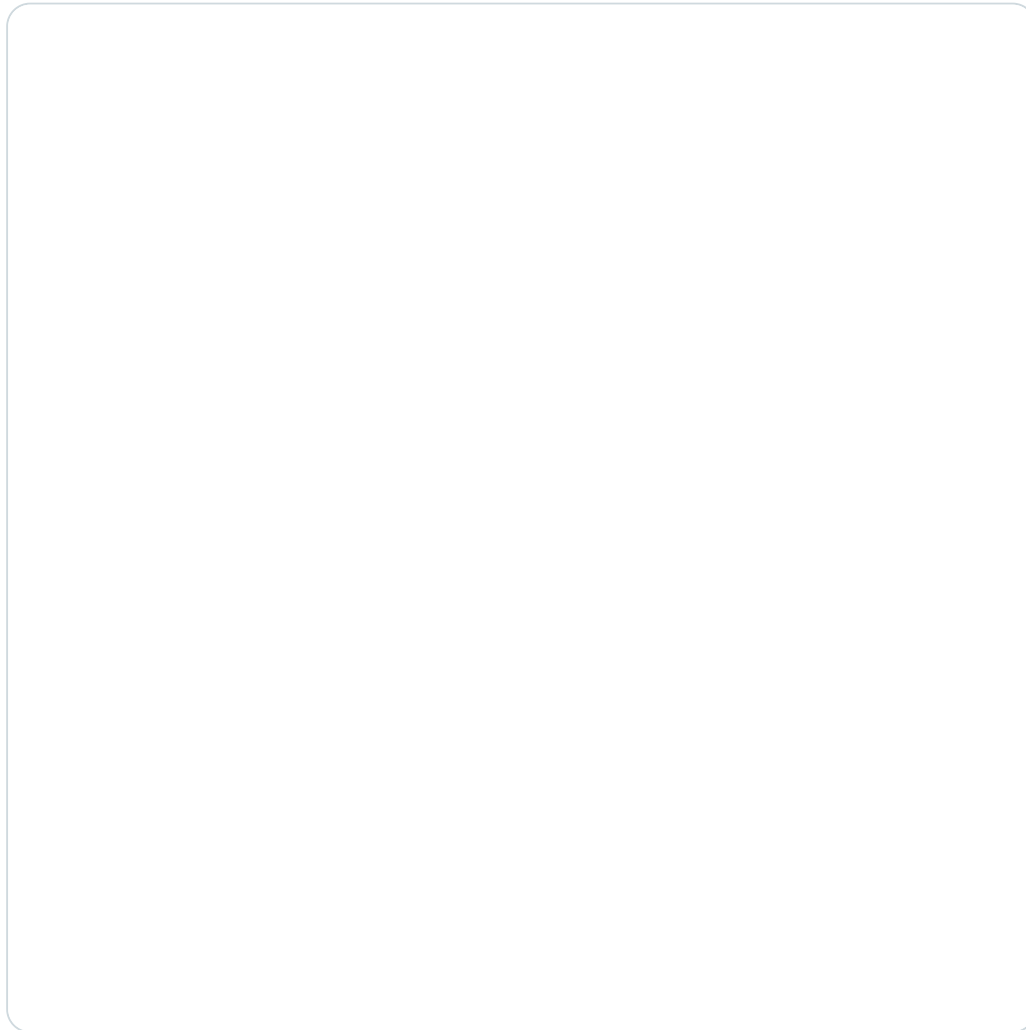
@InstagramComms · [Follow](#)

We're working to keep the Instagram community safe and informed on COVID-19. Here's an update on some of the changes we've made so far:

Instagram Comms 

@InstagramComms · [Follow](#)

We're removing known harmful misinformation related to COVID-19, and when someone taps on a hashtag related to COVID-19, we show resources from [@WHO](#), [@CDC](#) and local health authorities.



12:43 PM · Mar 6, 2020



433



See the latest COVID-19 information on Twitter

[Read 28 replies](#)

Instagram Comms 

· Mar 6, 2020 20392



@InstagramComms · [Follow](#)

Replying to @InstagramComms

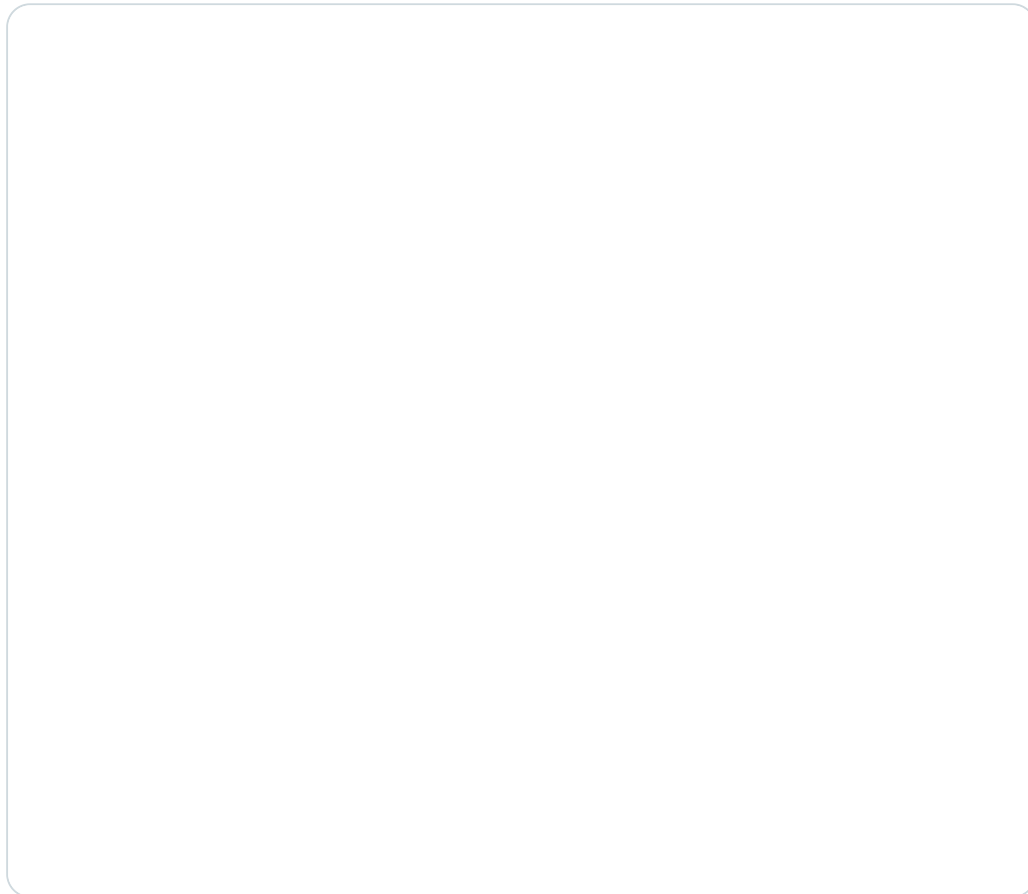
We're also:

- Sending posts that may be misleading to our fact-checking partners for review
- Blocking and restricting hashtags being used to spread misinformation
- Banning ads exploiting the situation

Instagram Comms 

@InstagramComms · [Follow](#)

Finally, we're thinking through a longer term solution to help connect people searching COVID-19 related terms with credible information. In the meantime, we're showing the accounts of leading health organizations in these searches to better connect people to credible resources.



12:43 PM · Mar 6, 2020



241

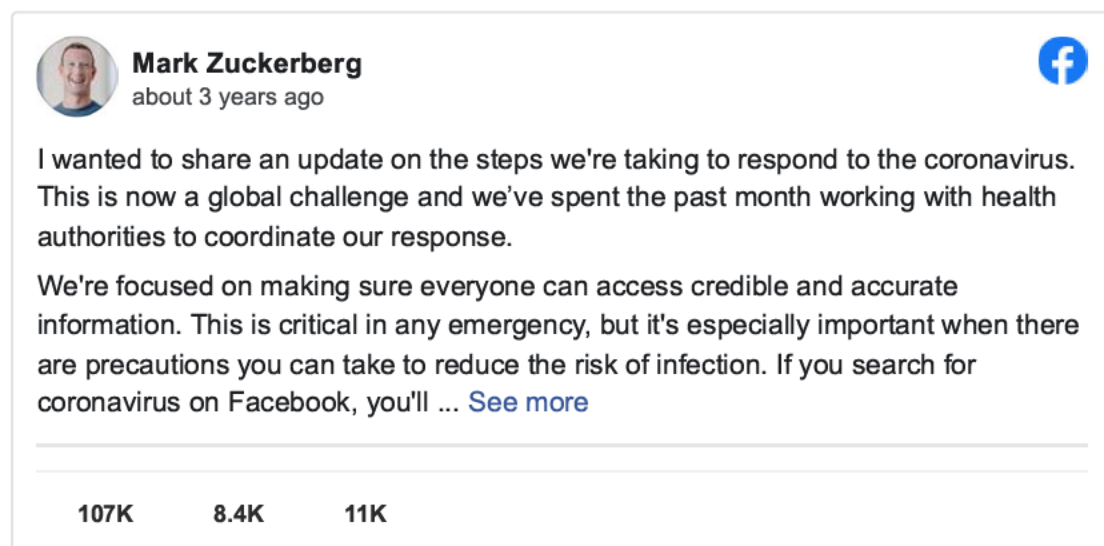


See the latest COVID-19 information on Twitter

[Read 22 replies](#)

Supporting Global Health Organizations With Free Ads and More

CEO Mark Zuckerberg posted about the latest steps Facebook is taking.

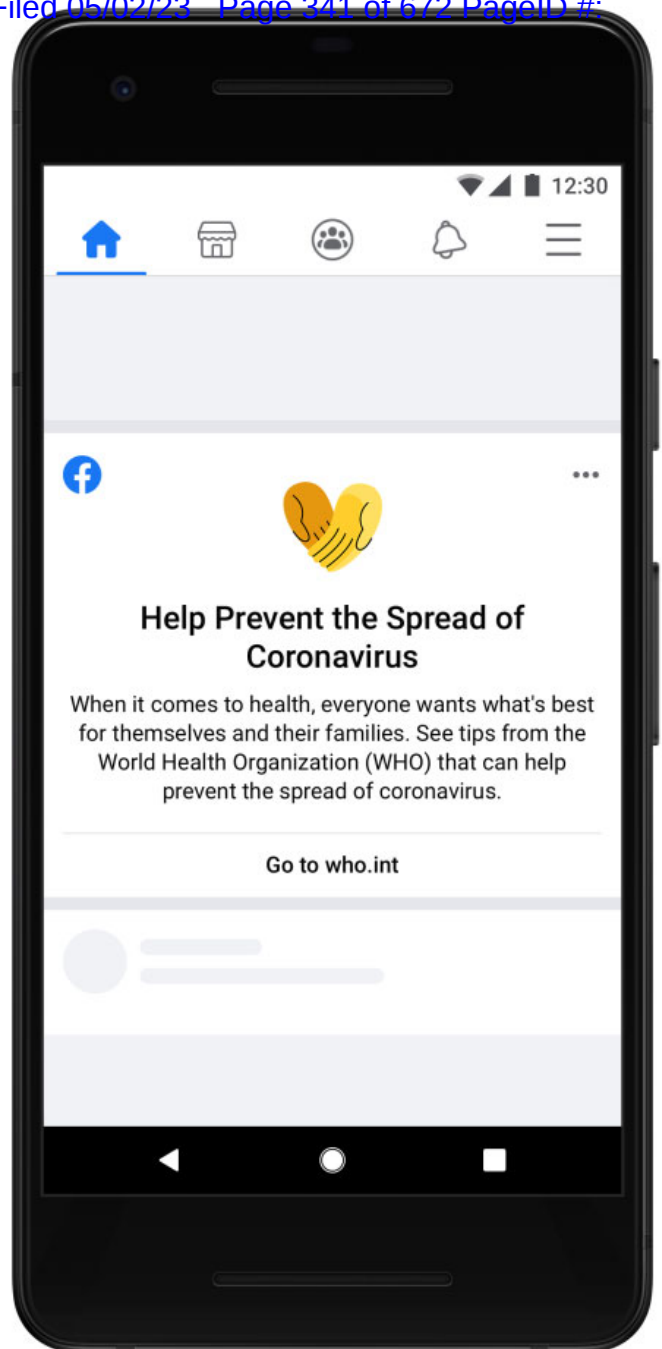
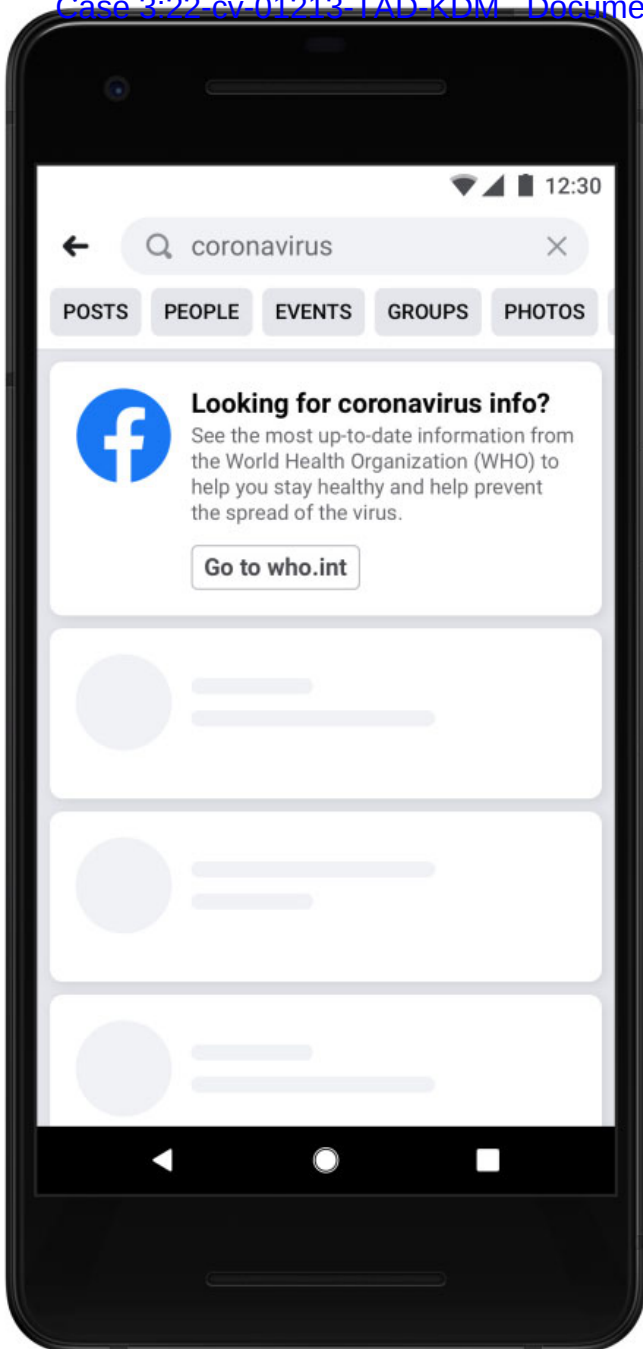


Update on February 26, 2020 at 7:13PM PT:

As world health officials issue new guidance and warnings about coronavirus (COVID-19), we're continuing our work to connect people to information from regional and local health organizations and limit the spread of misinformation and harmful content about the virus.

Connecting People to Accurate Information and Helpful Resources

Anyone who searches for information related to the virus on Facebook is shown educational pop-ups on top of search results connecting them to expert health organizations including the World Health Organization (WHO). We've launched these globally over the last few weeks in all languages on Facebook, directing people to the WHO. In several countries we are directing people to their local ministry of health. For example, in the US we are directing people to information from the Centers for Disease Control and Prevention (CDC) and in Singapore, we're directing people to the Singapore Ministry of Health. Moreover, in countries where the WHO has reported person-to-person transmission and deaths, we've shown additional messages to people toward the top of News Feed with more information.



Exploitative Tactics in Ads

Yesterday we put a new policy into effect to protect people from those trying to exploit this emergency for financial gain. This means we are now prohibiting ads for products that refer to the coronavirus in ways intended to create a panic or imply that their products guarantee a cure or prevent people from contracting it. For example, ads for face masks that imply they are the only ones still available or claim that they are guaranteed to prevent the virus from spreading will not be allowed to run on our platforms.

Today, the World Health Organization (WHO) declared the coronavirus a public health emergency of international concern. As the global public health community works to keep people safe, Facebook is supporting their work in several ways, most especially by working to limit the spread of misinformation and harmful content about the virus and connecting people to helpful information. Here are some specific steps we are taking.

Limiting Misinformation and Harmful Content

Our global network of third-party fact-checkers are continuing their work reviewing content and debunking false claims that are spreading related to the coronavirus. When they rate information as false, we limit its spread on Facebook and Instagram and show people accurate information from these partners. We also send notifications to people who already shared or are trying to share this content to alert them that it's been fact-checked.

We will also start to remove content with false claims or conspiracy theories that have been flagged by leading global health organizations and local health authorities that could cause harm to people who believe them. We are doing this as an extension of our existing policies to remove content that could cause physical harm. We're focusing on claims that are designed to discourage treatment or taking appropriate precautions. This includes claims related to false cures or prevention methods — like drinking bleach cures the coronavirus — or claims that create confusion about health resources that are available. We will also block or restrict hashtags used to spread misinformation on Instagram, and are conducting proactive sweeps to find and remove as much of this content as we can.

Providing Helpful Information and Support

Our platforms are already being used to help people connect with accurate information about the situation, including from global and regional health organizations. We've been closely coordinating with leading health organizations to make this easier and more accessible for people using Facebook and Instagram.

For example, we will help people get relevant and up-to-date information from partners through messages on top of News Feed on Facebook; these will be deployed based on guidance from the WHO. When people search for information related to the virus on Facebook or tap a related hashtag on Instagram, we will surface an educational pop-up with credible information. We have also provided free advertising credits to enable organizations to run coronavirus education campaigns on Facebook and Instagram in affected regions and are discussing ways to provide additional assistance and support to health authorities.

Empowering Partners with Data Tools

We are empowering leading researchers at Harvard University's School of Public Health and National Tsing Hua University in Taiwan by sharing aggregated and anonymized mobility data and high resolution population density maps to help inform their forecasting models for the spread of the virus as part of our broader Data for Good program. We may expand these efforts to a broader set of partners in the coming weeks. We are also helping partners understand how people are talking about the issue online through tools like CrowdTangle to better inform their efforts.

Not all of these steps are fully in place. It will take some time to roll them out across our platforms and step up our enforcement methods.

We will provide updates on additional steps we are taking in coordination with global and regional partners as the situation continues to evolve.

Categories:

Company News, Integrity and Security, Meta,
Safety and Expression



Tags:

Combating Misinformation, COVID-19 Response,
Data for Good, False News, Health

RELATED NEWS

Topics
Facebook

Company News

Supporting Muslim Mothers

Nafisa Razaes Facebook Fundraisers to support

other Muslim mothers.

April 28, 2022

- Technology and Innovation
- Data and Privacy
- Safety and Expression
- Combating Misinformation
- Economic Opportunity
- Election Integrity
- Strengthening Communities
- Diversity and Inclusion

Featured News

Instagram

New Features on Instagram Reels: Trends, Editing and Gifts

April 14, 2023

Meta Quest

Peacock on Meta Quest: Stream Current Movies, Hit TV Shows and Live Sports in VR

April 12, 2023





Virtual reality



Smart glasses



About us



Our community



Our actions



Support



Community Standards

| Data Policy

Terms

| Cookie policy

United States (English) ▼

DEFENDANTS' EXHIBIT 145:



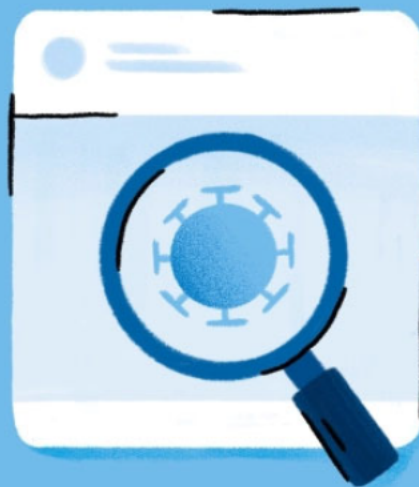
[Back to Newsroom](#)

Meta

How We're Taking Action Against Vaccine Misinformation Superspreaders

August 18, 2021

By Monika Bickert, Vice President, Content Policy



19 vaccine misinformation can be solved simply by removing 12 people from social media platforms. People who have advanced this narrative contend that these 12 people are responsible for 73% of online vaccine misinformation on Facebook. There isn't any evidence to support this claim. Moreover, focusing on such a small group of people distracts from the complex challenges we all face in addressing misinformation about COVID-19 vaccines.

That said, any amount of COVID-19 vaccine misinformation that violates our policies is too much by our standards — and we have removed over three dozen Pages, groups and Facebook or Instagram accounts linked to these 12 people, including at least one linked to each of the 12 people, for violating our policies. We have also imposed penalties on nearly two dozen additional Pages, groups or accounts linked to these 12 people, like moving their posts lower in News Feed so fewer people see them or not recommending them to others. We've applied penalties to some of their website domains as well so any posts including their website content are moved lower in News Feed. The remaining accounts associated with these individuals are not posting content that breaks our rules, have only posted a small amount of violating content, which we've removed, or are simply inactive. In fact, these 12 people are responsible for about just 0.05% of all views of vaccine-related content on Facebook. This includes all vaccine-related posts they've shared, whether true or false, as well as URLs associated with these people.

The report upon which the faulty narrative is based analyzed only a narrow set of 483 pieces of content over six weeks from only 30 groups, some of which are as small as 2,500 users. **They are in no way representative of the hundreds of millions of posts that people have shared about COVID-19 vaccines in the past months on Facebook.** Further, there is no explanation for how the organization behind the report identified the content they describe as “anti-vax” or how they chose the 30 groups they included in their analysis. There is no justification for their claim that their data constitute a “representative sample” of the content shared across our apps.

Focusing on these 12 individuals misses the forest for the trees. We have worked closely with leading health organizations since January 2020 to identify and remove COVID-19 misinformation that could contribute to a risk of someone spreading or contracting the virus. **Since the beginning of the pandemic across our entire platform, we have**

Case 3:22-cv-01213-TAD-KDM Document 264-7 Filed 05/02/23 Page 350 of 672 PageID #: 29403
removed over 3,000 accounts, Pages and groups for repeatedly violating our rules against spreading COVID-19 and vaccine misinformation and removed more than 20 million pieces of content for breaking these rules.

None of this is to suggest that our work is done or that we are satisfied. Tracking and combating vaccine misinformation is a complex challenge, made more difficult by the lack of common definitions about what constitutes misinformation, and the reality that guidance from scientific and health experts has evolved and will continue to evolve throughout the pandemic. That's why we're continuing to work with external experts and governments to make sure that we are approaching these issues in the right way and making adjustments if necessary. In the meantime, we will continue doing our part to show people reliable information about COVID-19 vaccines from health experts and help people get vaccinated.

Categories:

Integrity and Security, Meta, Public Policy, Safety and Expression



Tags:

Combating Misinformation, COVID-19 Response

RELATED NEWS

Meta

Meta Asks Oversight Board to Advise on COVID-19 Misinformation Policies

We're asking the Oversight Board whether our current COVID-19 misinformation policy is still appropriate.

July 26, 2022

Topics

Company News

Technology and Innovation

Data and Privacy

Safety and Expression

Combating Misinformation

Economic Opportunity

Election Integrity

Strengthening Communities

Diversity and Inclusion

Featured News

Instagram

New Features on Instagram Reels: Trends, Editing and Gifts

April 14, 2023

Meta Quest

Peacock on Meta Quest: Stream Current Movies, Hit TV Shows and Live Sports in VR

April 12, 2023





Virtual reality 

Smart glasses 


About us 

Our community 

Our actions 

Support 

[Community Standards](#) | [Data Policy](#) | [Terms](#) | [Cookie policy](#)

United States (English) 

DEFENDANTS' EXHIBIT 146:



Tweet



Robert F. Kennedy Jr 
@RobertKennedyJr



[#HankAaron](#)'s tragic death is part of a wave of suspicious deaths among elderly closely following administration of [#COVID](#) [#vaccines](#). He received the [#Moderna](#) vaccine on Jan. 5 to inspire other Black Americans to get the vaccine. [#TheDefender](#)



childrenshealthdefense.org

Home Run King Hank Aaron Dies of 'Undisclosed Cause' 18 Days After Recei...
The 86-year-old sports icon received the first of two doses of Moderna's vaccine on Jan. 5, in an attempt to inspire other Black Americans to step up t...

5:41 PM · Jan 22, 2021

6,554 Retweets 1,885 Quotes 9,777 Likes 447 Bookmarks



JulietYelverton Telg <https://t.me/Julie...> @healing... · Jan 22, 2021



The father of a friend died after a vaccine yesterday



25



7



86



TheRealMichaelScott   ...  @MikeScottNew... · Jan 23, 2021



Don't miss what's happening

People on Twitter are the first to know.

Log in

Sign up



sean @spiderkemp · Jan 22, 2021

The elderly tend to die. Sometimes after a vaccine, sometimes after brushing their hair, or drinking coffee. Maybe it was the hair brushing or the coffee.

64 8 417



Don Tomasso @Tomaseetoo · Jan 22, 2021

you could say the same thing about the elderly that apparently died from covid. the CDC stated that 96% of people that died from covid actually had at least 3 other probable causes of death on their certificate. some even died from car accidents but were positive at the time.

7 2 21

[Show replies](#)



Shel Holtz @shelholtz · Jan 22, 2021

Jumping to conclusions is part of the anti-vaxxer playbook. Just stop.

19 10 511



Keyhole @keyholeopa · Jan 8

I call it logical thinking.

1 1 21 1,271

[Show replies](#)



Yashar Ali @yashar · Jan 22, 2021

You are a danger to public health and a disgrace to your family. A reckless and horrible man.

I'm glad some of your family members have condemned your anti-science rhetoric.



Don't miss what's happening

People on Twitter are the first to know.

[Log in](#)

[Sign up](#)



nytimes.com

Opinion | Vaccines Are Safe, No Matter What Robert Kennedy Jr. Say...
I love my uncle. But when it comes to vaccines, he is wrong.



227



675



6,780



Joe Colangelo  @Itsjoeco · Jan 23, 2021

...

Kennedies going to Kennedy.



E. Ayobiojo @GrantMamba · Jan 22, 2021

...

Bobby you're better than this. Hank passed away in his sleep after 86 years on this earth. Don't continue this notion.



47



16




1,078



MrsLakey @MissusLakey · Jan 22, 2021

...

How dare you make assumptions to push your anti-vax agenda. This is grossly irresponsible 



28



30



1,163



 **TheKitty**   @ZeroDarkKitty · Jan 23, 2021

...

Larry King is dead today - He took the Vax

49 dead in Norway - they stopped giving it

Oh, HEY ... see where the CDC is now saying that 96% of COVID positives were WRONG due to the BAD TESTS?

Gov "Whitler" has re-opened MI as of Feb 1st

This is not a pandemic

Wake up



1



11



Don't miss what's happening

People on Twitter are the first to know.

Log in

Sign up



Don't miss what's happening
People on Twitter are the first to know.

Log in

Sign up

DEFENDANTS' EXHIBIT 147:

MAY 05, 2021

Press Briefing by Press Secretary Jen Psaki and Secretary of Agriculture Tom Vilsack, May 5, 2021

James S. Brady Press Briefing Room

12:32 P.M. EDT

MS. PSAKI: Hi, everyone.

Q Hi, good afternoon.

MS. PSAKI: Good afternoon. Okay. We have another special guest joining us today: Secretary of Agriculture Tom Vilsack.

As you all know, this is Secretary Vilsack's second turn at the Department of Agriculture, which he led in the Obama-Biden administration from 2009 through 2017, making him the longest-serving member of President Obama's Cabinet.

In those years, Secretary Vilsack fought to put Americans back to work by investing in rural infrastructure, renewable energy, and large-scale conservation partnerships. Under his leadership, USDA introduced healthier food choices in school meals to benefit 50 million children, and expanded free and reduced-price lunches for millions of kids.

Prior to his appointment — or nomination and confirmation, I should say — Secretary Vilsack served two terms as the Governor of Iowa, in the Iowa State Senate, and as the Mayor of Mount Pleasant, Iowa.

With that, I will turn it over to the Secretary, who will be — take a few questions once he concludes his remarks.

SECRETARY VILSACK: Jen, thanks very much. It's certainly a pleasure to be here today with all of you.

I'm here primarily to talk about food and nutrition security. And you may think that that is just about food and nutrition security, but, in fact, it's about a lot more than that.

When you understand that 25 percent of America's workforce is directly or indirectly impacted by the food and ag industry, that it represents a significant percentage of our GDP, that educational achievement is somewhat dependent on youngsters having healthy and nutritious food as they begin their school year and school day, and the fact that it is a noted effort in reducing poverty, food and nutrition security becomes an important issue. And certainly, we've seen the impact of that during the course of the pandemic.

When the American Rescue Plan was enacted, hunger in the United States was at 14 percent of our population, which was an incredibly high number. Today, as a result of the investments under the American Rescue Plan, we now know that hunger has dipped to 8 percent of America's population. That's a remarkable drop in a six-month period.

It is a result of extending SNAP, as we did in the American Rescue Plan; creating a Summer EBT program that will institute opportunities for nearly 30 million children to have access to nutrition during the summer months; increasing our commitment to WIC; and basically making a down payment, if you will, on hunger reduction.

We have the opportunity, over the course of the next several months, as Congress considers the American Jobs Plan and the American Family Plan, to cement those — those results and to actually build upon them.

There are three key investments for nutrition and food security in the American Families Plan. First, we are going to make permanent this incredible and historic effort to feed kids during the summer months. There are, as I said, nearly 30 million American children who are in free-and-reduced-lunch status in schools.

At the end of the school year, there is no program, other than the summer feeding program, which impacted and affected several million of those 30 million children. Now we have the opportunity to provide each one of these families with a card that looks like this.

This is the Summer EBT card that's available. It allows parents the opportunity to go to the grocery store — as they do with their SNAP card — and be able to purchase additional fruits and vegetables and other wholesome food for their children, ensuring that 30 million kids will have the opportunity to have nutrition during the summer, which means that they'll be better prepared to begin school ready to learn in the fall.

We're also extending, with this effort, the opportunity to impact free school meals in high-poverty school areas by focusing on the Community Eligibility program that essentially identifies the ability of a school district where SNAP participation is roughly 40 percent to extend free meals to everyone in that school.

This is going to expand opportunities for youngsters to be well fed. And we know from a recent Tufts study that one of the healthiest places in the country for children to eat is now in America's schools. So we're going to see that extended, and we're going to focus — with a specific, laser-like focus — on elementary schools to make sure that our youngest learners have the best possible opportunity.

And finally, we're going to invest a billion dollars, with Congress's help and assistance, in trying to figure out strategies that will improve, even more than we already have, the nutritional value and quality of the meals that youngsters receive in schools.

So, these three steps — these three key investments of the American Families Plan will allow us to cement the gains under the American Rescue Plan and, hopefully, impact and reduce hunger to the point, eventually, one day, where we won't have to have a press conference about — about hunger.

So, with that, I'd be happy to take questions.

MS. PSAKI: Great. Andrea, do you want to kick us off?

Q Yeah. Secretary Vilsack, a couple questions. One about the mines that you — the mine project that you had previously blocked, and then the Trump administration allowed those to open up. Do you have any particular view on whether that should be reopened or not? This is the Twin Metals copper mine.

SECRETARY VILSACK: There's always a very difficult balance to strike in any of these questions. And certainly, in this particular one, you're balancing a pristine, incredibly important, and valuable natural site — the Boundary Waters of the Mississippi, a tremendously unique area. It's one that the late Walter Mondale felt very strongly about, and I know that from a personal experience with the former Vice President. He called me repeatedly on this issue.

So, you've got that on one hand. On the other hand, you obviously have jobs and economic

opportunity. And I think the challenge is to try to see if you can strike a balance. And that's what we attempted to do in the previous administration, and I don't see any reason why we should — why we should change that calculation: trying to find the balance between preserving a pristine area and, at the same time, looking for ways in which job growth, economic growth can take place in rural areas. And that's what we're going to attempt to do.

There are no final decisions being made on this. This is obviously something we also have to do in conjunction with the Department of Interior. They have a stake in this issue as well.

Q (Inaudible.)

MS. PSAKI: Alex — oh, I just want to get to a bunch of people, and he has limited time. So, go ahead, Alex.

Q Sure. One way of increasing SNAP benefits is by reforming the Thrifty Food Plan, and I know that that is under review right now. Can you talk a little bit about what that review entails, and when we should expect results, and how the reforms would be implemented if the program is (inaudible)?

SECRETARY VILSACK: It's a complicated question, and one that hasn't been reviewed in detail for quite some time. And we expect and anticipate, during the course of the summer months, that we will complete our review and then have an opportunity, perhaps, to have a conversation about this in the fall.

And this will be appropriately timed because, as you know, the American Rescue Plan called for an extension of the increase in SNAP over the course of the summer months until the end of September. So it's timely for us to look at this.

I'd simply say that the principles that we're operating under in this area are:

Number one, that the benefit has to be meaningful to families — American families. With the American Rescue Plan, we saw an additional \$100 a month for a family of four being added to the groceries — to their grocery purchases.

It also impacts jobs. As I said before, that SNAP benefit increased and supported tens of thousands of jobs in grocery stores and across the food chain.

It also has to be conveniently available. It's one of the reasons why, again, the American

Rescue Plan has provided opportunities for us to look at online purchasing — make it more convenient.

It has to be operated with integrity, obviously.

And it has to be — we have to look for ways in which we can incent and encourage those dollars to be used in the best way possible to provide the most nutritious benefit to American families.

And that's the goal, and that's what we'll look at when we look at the Thrifty Food Plan.

MS. PSAKI: Alex.

Q Secretary, a group of Midwestern farmers, last week, sued over the COVID — a COVID loan forgiveness program, arguing that it's unfair to them because they're white. Your reaction to that lawsuit? And do you stand by the program's structure?

SECRETARY VILSACK: That's a great question. I appreciate it. I think I have to take you back 20, 30 years, when we know for a fact that socially disadvantaged producers were discriminated against by the United States Department of Agriculture. We know this.

We have reimbursed people in the past for those acts of discrimination, but we've never absolutely dealt with the cumulative effect. And by "cumulative effect," I mean this: When I have the full advantage of all the USDA programs throughout the last 30 years, my operation could grow. I could invest in more land. I could get the latest and best technology. I could plant my crop at just the right time. I could make more money. If I had limited access or no access to USDA programs, obviously my operation — significantly limited.

So, the American Rescue Plan's effort is to begin addressing the cumulative effect of that discrimination in terms of socially disadvantaged producers.

Secondly, when you look at the COVID relief packages that had been passed and distributed by USDA prior to the American Rescue Plan, and you take a look at who disproportionately received the benefits of those COVID payments, it's pretty clear that white farmers did pretty well under that program because of the way it was structured. It's structured on size; it's structured on production.

So I think there is a very legitimate reason for doing what we are doing. I think it has to be

complemented with additional steps, which the American Rescue Plan provides — an equity commission to take a look at whether or not there are systemic barriers that need to be removed at the Department.

And — and also, taking a look at how we might be able to create better technical assistance, better access to land, better access to markets for socially disadvantaged producers and for local and regional food production.

So we're going to continue to proceed forward. Understand that litigation is going to be what it is, and we're wal- — we'll obviously have the Department of Justice and others do what they do. An- — but in the meantime, the U.S. Department of Agriculture is going to move forward with that effort.

MS. PSAKI: Kristen.

Q Thank you, Secretary Vilsack. You've just outlined the plans for the ARP funds through the fall to deal with some of the issues around hunger. How long do you anticipate those funds will last, particularly given that next year's schoolyear will be unique — coming off of a year where most schools have been closed for the better part of the year? And will you need more funds from Congress to address this (inaudible)?

SECRETARY VILSACK: Well, I think that's one of the reasons why the President proposed the American Families Plan as a continuation and as — allowing us to basically cement and make more permanent the gains that we've seen from the American Rescue Plan.

In the meantime, we have worked with schools, understanding they are faced with a lot of uncertainty about the upcoming schoolyear. And so we have already decided that we have available resources to be able to provide for universal free lunch for schools throughout the '21-'22 schoolyear. And that will extend, I think, until the end of June 2022.

With the passage of the American Families Plan, we would then have the Summer EBT program to provide additional support and help. And that would give us, I think, enough lead time for school districts to be able to adjust back to what the new normal will be.

In the meantime, we'll be looking at, hopefully, the use of the pilot under the American Rescues — under the American Families Plan, to see if there are ways in which we can incent additional nutritional value for those meals. And we'll be using, hopefully, with the passage of the American Families Plan, a more targeted effort in high-poverty schools — elementary

Q Thank you, Secretary.

MS. PSAKI: Kaitlan. That will be the last one.

Q On this idea of a carbon bank, since you've been on the job, what is the feedback that you've gotten from farmers? And is this something that you think needs congressional approval?

SECRETARY VILSACK: You know, I was at a meeting yesterday with the Environmental Protection Agency Administrator, Michael Regan. He did a terrific job. We had probably 25 farmers.

I was very pleased with the level of support and interest that the farm community has for ways in which they can be engaged in this effort to reduce emissions and to be engaged in this climate effort.

We had multiple questions about this in terms of "How can we do this?" — not "We're against it" or "We are opposed to it" or "We don't think it should happen." It was, "How can we do this? How can we be part of this?"

Because farmers understand something very, very fundamental about this: This is the opportunity of a lifetime for us to create additional revenue opportunities for farmers. Now, why is that important? Because today, 89.6 percent of American farms — the majority of income does not come from the farm for those farm families. That means they have to have an off-farm income.

So it's the Department of Agriculture's job to find more, better, and new markets. Climate provides that opportunity. Whether it's a fund or whether it's conservation resources, whether it's investments in technology that will allow them to capture methane and reuse it, or whether it's creating new opportunities for bioprocessing and new jobs in rural places, all of that has to be done.

And I think the USDA has — has enormous capacity, an enormous set of tools that can be used to provide the resources to work with the farm community to embrace this future. And I think they are in agreement with President Biden when he says the net goal here is net-zero emissions by 2050. I think that's doable. And I think in doing it, I think we'll improve income opportunities for farmers, we'll certainly do right by the environment, and I think we'll also

Q Would it need congressional approval — a carbon bank?

SECRETARY VILSACK: Well, it needs congressional approval in the sense that you have resources in all of these programs that require funding. We have a lot of flexibility already at USDA, and we're going to be utilizing that flexibility in a way that creates more, new, and better markets. And I think farmers are going to find that to be a very — they're going to be very agreeable with that.

Q Thank you.

MS. PSAKI: Thank you, Secretary Vilsack. And as always, if you all have follow-up questions, we are happy to connect you with his team following the briefing.

SECRETARY VILSACK: Great.

MS. PSAKI: Thank you. And we'll love to have you back.

SECRETARY VILSACK: You bet. I'll take my notes. Appreciate it.

MS. PSAKI: Thank you so much.

I'll just note my first campaign was for the Secretary's gubernatorial race in 2002, so full circle.

A couple of items — additional items for all of you at the top. This afternoon, President Biden, as you know, will deliver remarks on Amer- — the American Rescue Plan's Restaurant Revitalization Fund — the administration's program to provide relief to restaurants, bars, food trucks, and other food and drink establishments.

As we all know, restaurants were some of the first- and worst-hit businesses in the pandemic. The Restaurant Revitalization Fund provides \$28.6 billion in direct relief to restaurants and food and beverage establishments, and prioritizes those that are women-owned, veteran-owned, and owned by other socially and economically disadvantaged individuals by only funding applications from these businesses for the first 21 days of the program. Then it expands beyond there.

Earlier today, the President also visited one local restaurant that was a beneficiary of relief

funding through the Revitalization Fund's pilot program. Taqueria [Las] Gemelas — I'm going to butcher that and I apologize; I want to go there and have some tacos — is owned in part by Mexican immigrants and, during the pandemic, went from 55 employees to just 7. So clearly, in great need.

These funds will allow business owners to complete delayed projects, rehire and raise the wages of their staff, pay their rent, and operate with confidence again. Applications for the program opens up on Monday. And in just the first two days of the program, 186,200 restaurants, bars, and other eligible businesses in all 50 states; Washington, D.C.; and 5 U.S. territories applied for relief.

Ninety-seven thousand six hundred applications came from restaurants, bars, and other eligible businesses owned and controlled by women, veterans, socially and economically disadvantaged individuals, or some combination of the three.

Sixty-one thousand seven hundred applications came from businesses with under \$500,000 in annual pre-pandemic revenue, representing some of the smallest restaurants and bars and businesses in America. And we look forward to implementing that program.

With that, I think we can go, Alex, to you. Questions.

Q So the CDC's summer camp guidance is very strict. As Dr. Fauci acknowledged today, it requires even adults who have been vaccinated to wear masks outside at all times. It requires children to be socially distanced. Can you explain why that contradicts the administration's guidance that vaccinated adults don't have to wear masks outside?

And also, Dr. Fauci suggested that it may change as the science becomes clear, but are — is the administration at all concerned that there won't be compliance with something this strict and there won't be compliance if it continuously changes?

MS. PSAKI: Sure. Well, first, I think everyone can expect that the guidance will continue to be updated and will continue to change. And I think, as a parent myself of kids going to summer school — not summer school, summer camp; don't tell them I said that — (laughter) — you know, they — I would welcome that.

And there's no question what the CDC is trying to do is provide guidance to the American public — to parents, to families — that they can trust, that they know is reliable — based on medical experts, doctors; based on data — on how they can feel safe. The guidance that was r-

— that was rolled out last week does not convey that when you're outside in a crowd, you cannot — you should not wear a mask.

If you're outside and you're not in a crowd, then you — and you're vaccinated, you don't need to wear a mask. Obviously, there is nuance in all of these applications, and people are still learning how to apply it.

But as kids are dropping off — as parents, I should say, are dropping off their kids at summer camp; as there are tons of kids, tons of parents, counselors — you know, that certainly wouldn't — wouldn't be someone alone.

But I think what Dr. Fauci was conveying, Alex, is that the data — they're going to continue to look at the data. And they want to put out updated guidance as they feel comfortable and confident in what they can provide to the American public.

Q Sure. And there's a new evaluation of the American Families Plan out by the Penn Wharton Budget Model. And they found, actually, that the plan would increase the deficit and fail to grow the economy as much as President Biden has claimed.

And so it's — is there a risk, in the long term, that the President might not be able to fully deliver on what he's promised economically?

MS. PSAKI: Well, first, let me say we strongly agree — disagree with the analysis, as do other independent experts.

According to an analysis out this week from Moody's, GDP in 2030 will be more than \$700 billion higher than it would be without the Jobs and Family — the Jobs Act — the Jobs Plan and the Families Plan.

This is in large part because labor force participation will be nearly a full percentage point higher due to the effects of the benefits of childcare support — child support — childcare support and paid family leave. And that same analysis found that the economic benefits would only increase over time due to increased college enrollment and universal pre-K, which will help some of the 2 million women who are no longer in the workforce get back in.

The Penn Mo- — Wharton Model analysis is also off in a number of important ways. It gets the cost of the investments wrong by about \$700 billion, even though our estimates come from career officials at OMB. Moody's, for example, arrived at deficits even lower than the

administration when — than we had when it came to the effect of the Families Plan.

And, of course, our plan would be implemented over a series of 8 years and 10 years, and paid for over 15. So, we're going to rely on the majority of economic analysis out there and our own analysis in here. And we are confident we'll be able to reach both our job creation projections and, of course, do it in a way we can pay for it.

Q And one international question: Israeli Prime Minister Benjamin Netanyahu missed the deadline to put together a coalition government yesterday — or a new governing coalition. Is the President monitoring this situation? And does the administration have any sort of response or perspective on the possibility of a new coalition government there?

MS. PSAKI: Well, we do read all of your news coverage, but we are not going to comment publicly on government formation while that process is underway.

Go ahead, Andrea.

Q Okay, there are a couple follow-ups on Vilsack's answer — Secretary Vilsack's answer on the Twin Metals thing. Is that a decision that you think will be coming at any point soon? Or is that just, sort of, carved out?

MS. PSAKI: I don't have a prediction of that. I would say I would refer you to the Department of Agriculture. And they would, of course, be the right source for that information. We can see if there's more follow up on it, on the timeline.

Q Okay. And then, on the issue of the G7 meeting and the subsequent meetings group — Putin. Have you — do you have any news for us on that front, in terms of timing and also the agenda?

MS. PSAKI: Not quite yet. As soon as we have details or any confirmed details of timing, location, date, participation, we will of course share that with you. And I would expect we wouldn't have more specifics on an agenda, if and when we have it confirmed, until much closer.

Q And then just one more on my favorite topic of the WTO.

MS. PSAKI: Oh, I don't know which one it is.

Q TRIPS waivers.

MS. PSAKI: Okay.

Q TRIPS wai- — (laughter.) TRIPS waivers.

MS. PSAKI: Mm-hmm.

Q So, this morning there was a meeting of the WTO. Katherine Tai made some comments during an FT session talking about, you know, time being of the essence — really, sort of, underscoring.

There are multiple reports out, also, about, kind of, a division within the administration on this waiver issue. Can you just really walk us through what your perspective is on this and why?

So the — there's so many people in institutions and organizations now really putting pressure on President Biden to back this waiver.

MS. PSAKI: Well, I think it's important, first, to just take a step back and remind everyone that President — the President spoke about his support for this type of a waiver back during the campaign.

But it — we are running a process — we have been running a process in the administration that includes all stakeholders in the administration. And he is somebody who has welcomed people of different views. He wants to know the details. He's a details guy, and he wants to dig into the pros and cons and all of the considerations for any decision.

As we look at this decision, what we're really talking about — I know you know this, Andrea, but for others — we're really talking about the U.S. position as it relates to the WTO process, right? And that process will take a series of months, and requires a unanimous point of view to move forward.

So what we are — the consideration now is — the U.S. position, our objective overall, as we look at this decision is: How can we provide as much supply in the most cost-effective way to the global community? And clearly, there are steps we've announced. We've take — we're in the process of taking — providing 60 million doses to the global community — once we have that available — that are AstraZeneca doses.

Earlier this week, Pfizer announced they'll also be sending doses, or manufacturing doses, for the global community. And we're going to continue to work with our partners. I expect we'll have more — now that the WTO meetings are underway, we'll have more to say very soon on this.

Q Are you concerned about setting a precedent that could be — so, even if India and South Africa narrow their proposal, which is apparently something that's going on — and maybe you could ask — you could — you could confirm that that is your understanding — even if that proposal is narrowed, are you concerned that you're going to be setting a precedent that could harm U.S. companies in the future — which is what, you know, we hear from U.S. industry?

MS. PSAKI: Well, clearly as these decisions are weighed, we take intellectual property incredibly seriously. And we also, though, are in the midst of a historic global pandemic, which requires a range of creative solutions. And we're looking at it through that prism.

Q It sounds — I'm sorry, Jen, I just want to be very clear. It sounds like you're pushing us or leaning towards some kind of a — a waiver of some kind.

MS. PSAKI: I'm not trying to give you an indication. That, obviously, would be an announcement or a decision that would be recommended by the USTR and a decision I would expect that would be made by the USTR. But what I'm trying to give you an understanding of, which I think was your question, is what the considerations are in the thinking and decision.

Q When do you think a decision will be made?

MS. PSAKI: Soon.

Go ahead.

Q I have questions on a couple of different topics. The first is on the debt limit: Is the White House concerned about being able to avoid a government shutdown and raising the debt limit considering the Treasury is unsure how long it can use the extraordinary measures it has? And what's the White House's strategy for pressuring Congress to agree to raise or suspended the debt limit? Or are you leaving that to Treasury to figure out?

MS. PSAKI: Well, first, I will say that, on the issue at hand, raising or suspending the debt ceiling does not authorize new spending. Sometimes — I'm not saying you're confused about that; some people sometimes are. It merely allows Treasury to meet obligations that Congress

has already approved. So, certainly, they would be in the lead, as they have historically been in most administrations, on making that case.

We expect Congress to act in a timely manner to raise or suspend the debt ceiling, as they did three times on a broad bipartisan basis during the last administration, including the same year that the former President signed into law tax cuts that added \$2 trillion to the deficit.

So, we certainly expect they will move forward, that this is something that has been done in a bipartisan basis; Democrats and Republicans have called for it in the past. And that's what we'll be advocating for.

Q Senate Minority Leader Mitch McConnell said this morning — when asked about, kind of, the issues within his own party — that, quote, “100 percent of my focus is on stopping this new administration.” And he touted, kind of, the unity within his caucus, from Susan Collins to Ted Cruz. Are you concerned that it will be difficult to work with Republicans when you're — when you have these kinds of statements coming from their Leader?

MS. PSAKI: Well, I guess the contrast for people to consider is 100 percent of our focus is on delivering relief to the American people and getting the pandemic under control and putting people back to work. And we welcome — support engagement and work with the Republicans on that. And there's — the President has extended an open arm to that. The door to the Oval Office is open. He's invited Senator Capito to bring a group of her choosing to the White House next week. And we think there is opportunity for agreement to deliver on — on relief to the American people.

Q Just one quick question: A judge, this morning, struck down the CDC's national moratorium on evictions. Do you have a response to that and the administration's plans to appeal, potentially?

MS. PSAKI: Yes, I do — we understand that it's just happened, as you alluded to, this morning. We understand the Department of Justice is reviewing the court's decision and should have more to say later today. We also recognize, of course, the importance of the eviction moratorium for Americans who have fallen behind on rent during the pandemic.

A recent study estimates that there were 1.55 million fewer evictions filed during 2020 than would be expected, due to the eviction moratorium. So it's clearly — has had a huge benefit. But we would expect that a response and any, of course, decision about additional action would come from DOJ. And you may hear more from them today.

Go ahead, Kristen.

Q Thanks, Jen. Facebook has decided to keep former President Trump off of its platform for now. Senator Ted Cruz tweeted the following: “For every liberal celebrating Trump’s social media ban, if the Big Tech oligarchs can muzzle the former President, what’s to stop them from silencing you?” What do you make of that comment? Does he have a point?

MS. PSAKI: Well, let me first say that this is an independent board’s decision, and we’re not going to have any comment on the future of the former President’s social media platform. That’s a decision that, it sounds like, the independent board punted back to Facebook to make in the next six months, as I know you all have reported.

The President’s view is that the major platforms have a responsibility related to the health and safety of all Americans to stop amplifying untrustworthy content, disinformation, and misinformation, especially related to COVID-19, vaccinations, and elections. And we’ve seen that over the past several months, broadly speaking. I’m not placing any blame on any individual or group; we’ve seen it from a number of sources.

He also supports better privacy protections and a robust anti-trust program. So his view is that there’s more that needs to be done to ensure that this type of misinformation; disinformation; damaging, sometimes life-threatening information is not going out to the American public.

Q You’re saying more that needs to be done. Are there any concerns though about First Amendment rights? And where does the White House draw the line on that?

MS. PSAKI: Well, look, I think we are, of course, a believer in First Amendment rights. I think what the decisions are that the social media platforms need to make is how they address the disinformation, misinformation — especially related to life-threatening issues like COVID-19 and vaccinations that are — continue to proliferate on their platforms.

Q I want to ask you, also, Jen, about police reform. President Biden said he wanted it done by the first anniversary of George Floyd’s death: May 25th. Is he confident that Congress can meet that benchmark? Where do those negotiations stand?

MS. PSAKI: Well, the negotiations are between members of Congress. So — and he, of course, is confident in the — those discussions and the work that is happening under the leadership of everyone from Congresswoman Karen Bass to Senator Cory Booker — obviously, Senator Tim

Scott, who he called out in his speech just last week.

And we are — we remain — we are in close touch with, of course, negotiators and kept abreast of their progress, but we will wait to see what comes out of those discussions.

Q If you do the math, though, this puts police reform, in some regard, ahead of the negotiations, one would think, for the American Families Plan, the infrastructure plan, which he set an end-of-the-summer deadline for. Is this now the President's top priority? Does he want Congress to tackle this first?

MS. PSAKI: Well, I would say that the President believes Congress can and should move forward with multiple policies at the same time. And, certainly, that — that is what is happening on Capitol Hill. I know those members who are playing central role — roles in these negotiations — and, obviously, they can speak to the frequency of the discussions and the status of them and we defer to them — they will be important participants, of course, in any outcome of negotiations around the American Jobs Plan, but those negotiations can happen simultaneously.

Q Just finally, Jen, how does he see his role? I mean, he's the one making this call to get this done. Has he reached out to Tim Scott — the person who's leading the charge on the GOP side?

MS. PSAKI: I don't have any calls or engagements to read out to you, but I can say that, as you know, a number of representatives of the families were here just last week, meeting with some senior members of the White House leadership.

The President has talked about how it's long overdue to put in place police reform measures — that that will help rebuild trust in our communities.

He used his joint session speech — the highest-profile moment in a first — in a President's first year — to talk about that and make the case.

And — but the negotiations are happening between members of Congress. He feels that's the appropriate place for them to be. And we will continue to use opportunities to call for this moving forward.

Go ahead, Kristin — Kristin? Kristen? Kristin? I got confused. Kaitlan.

Q There's a lot of "Ks." A lot of "Ks."

MS. PSAKI: There's a lot of "Ks." It's a Wednesday. Go ahead, Kaitlan.

Q That's all right. Kristin and I also have been dressing alike lately, so it's fine.

MS. PSAKI: Kristin has a very good mask on today. This Kristin. Both of your masks.

Go ahead, okay.

Q My question is on these restaurant funds.

MS. PSAKI: Yes.

Q When will they start being awarded? And does the President envision having to ask Congress for more money for this?

MS. PSAKI: Well, on the second piece — well, first, the first awards, as part of the pilot program, will be funded Friday. So —

Q Right. But for this program, not the pilot — the —the sec- — the actual part of it, not the pilot.

MS. PSAKI: Those who applied this week can expect up to — up to 14 days, on average, from submission to funding. So it will be a very rapid turnaround.

Q Okay. And does he envision asking Congress for more money for this?

MS. PSAKI: When Congress comes back, we are happy to discuss the best ways to further support small businesses, including restaurants hurt by the crisis. So he's certainly open to that.

And as I noted, there has already been a large interest in this program. And there are great needs across the country from these small businesses, from these restaurants that are in communities across the country.

So we will — we're happy to have a conversation with Congress about that.

Q Okay. And my question on the patents — you were talking about how the President, last

summer, expressed his favor for waiving these so countries would be able to mass produce these vaccines once they're ready. Of course, that was when they were not ready yet last summer.

MS. PSAKI: Yeah.

Q So, just to be clear: Is that still his position?

MS. PSAKI: That has been — that has been his position. He also believes that there needs to be an internal policy process. That's what's been ongoing.

The recommendation — the appropriate process — the recommendation to come from the USTR, and then any announcement about a decision would come from USTR. And that's how government should function and should work.

And as — and I noted, in response to Andrea's question — there are, of course, considerations, but we're also in the midst of a global pandemic, and we are — our objective is to getting as much supply out into the global community as — as quickly as possible and in the most cost-effective manner as we can.

Q But what did he communicate to Katherine Tai, his Trade Representative, before these meetings with the WTO on this are underway?

MS. PSAKI: Well, there have been discussions happening here in — through a policy process. I don't think his comments he made last summer are a secret. They're certainly not.

But, again, he's a believer that you need to have all parties at the table — everyone providing information, hearing details, pros and cons of every decision. And that's exactly what he asked for from his policy teams.

Q So given what he's heard from the policy teams, from the health experts — people like Dr. Fauci have weighed in publicly about whether this would be helpful in making vaccines right now or if that would be further down the road — but is it — is his position still what he said last summer, which is “absolutely, positively,” he will “ensure there are no patents [standing] in the way of other countries and companies' mass producing these lifesaving vaccines?”

MS. PSAKI: That has been his position, but he is the President of the United States, who believes in the advice, the counsel, the considerations of his policy teams. And that has been

the process that's been ongoing over the last several weeks. And I expect we'll have more to say quite soon.

It's also important to note, just — just in response to one of the things you said, that this is not — this would not be — this is about the U.S. position. There would be an entire process at the WTO that would be — likely be months in the making.

And that's just how the process works. So there's also a consideration leading up to that.

Q Okay. Thank you.

MS. PSAKI: Okay. Go ahead.

Q Thank you, Jen. Yesterday, you said that the CDC engaged with around 50 stakeholders when coming up with these guidelines for reopening schools.

MS. PSAKI: Yeah.

Q So, in addition to the teachers union — the American Federation of Teachers — who are these other roughly 50 stakeholders?

MS. PSAKI: Well, let me give you — I'm not going to read all 50 because, you know, but — and I'm happy to send them to you after.

But just as an example, while I find this lengthy list: You know, they include the YMCA. They include the Council of Chief State School Officers, the National Association of School Nurses, the National Governors Association, Big Cities Health Coalition, Autism Speaks, Council of Great City Schools.

So there's a range of organizations. And as we were talking about yesterday, the objective is to have a better understanding of implementation, how it would work, and ensure that these guidelines can be implemented and they would not provide harm to the communities that they would be impacting.

Q But can you just explain maybe just a little bit more — you know why the CDC needs all of this input from so many outside entities? Why can't it just come up with these science-based guidelines on its own?

MS. PSAKI: Well, they do so to ensure that the recommendations are feasible to implement and that they adequately address the safety and wellbeing of individuals the guidance is aimed to protect, and that type of consultation is pretty standard as a part of their consideration processes.

Q One other topic.

MS. PSAKI: Sure.

Q Right now, there is a huge Chinese rocket in outer space that's going to be crashing down to Earth, likely on Saturday, and nobody knows exactly where. It'll likely be in an ocean, but it could — or pieces of it could come down over a populated area, and this isn't the first time that China has allowed — knowingly allowed something like this to happen.

So does the White House condemn this kind of repeated reckless behavior from China's space program?

MS. PSAKI: Well, let me first say that U.S. Space Command is aware of and tracking the location of the Chinese Long March 5B in space. And obviously, the Space Command would have more specifics on that tracking and — and additional details.

The United States is committed to addressing the risks of growing congestion due to space debris and growing activity in space. And we want to work with the international community to promote leadership and responsible space behaviors. It's in the shared interests of all nations to act responsibly in space to ensure the safety, stability, security, and long-term sustainability of outer space activities.

So cooperation is a hallmark of our approach. We're going to work with our international partners on that. And certainly, addressing this is something we'll do through those channels.

Q And just a quick follow-up: If this rocket does cause some — some serious damages here on Earth, would the White House enforce China paying some sort of compensation as required by the U.N. Liability — Space Liability Convention?

MS. PSAKI: Well, again, I think we'd, of course, refer to the advice and guidance from U.S. Space Command and the Department of Defense and others. But we're not — at this point, we are certainly tracking its location through U.S. Space Command. And hopefully, that's not the outcome that we are working through.

Okay. Go ahead, Eli.

Q Thanks, Jen. Just interested if you have any response to some of the moves made this week by a few Republican governors to get rid of, you know, protections that were in place for people — public benefits, also public health restrictions — basically sending the message that the pandemic is over and sort of criticizing Washington — “the CDC bureaucrats,” as Ron DeSantis put it — for telling people they still need to wear masks indoors, those sorts of things — saying that the vaccines have worked.

How are you trying to thread that needle by celebrating the progress of all the people who have been vaccinated and keeping these things in place — and also trying to keep people from viewing this through a political lens? Any outreach to any of these Republican state officials about the message they’re sending? And any response to them from the podium?

MS. PSAKI: Sure. Well, first, we not only do a regular — a governors call every single week with governors from across the country, from red states and blue states, to talk about implementation, any changes we’re making to allocations — as we talked about just yesterday — but we also have regular engagement with governors and local officials about where the public health guidance is going, questions they have, and even sometimes challenges they have in their communities.

Our position, from the federal government, continues to be that the public health guidelines are in place to keep people safe — not just governors and leaders of states, of course, but people in communities, families, kids, people who are in vulnerable populations. And that we’ll continue to communicate that from the federal level, even as governors are pulling back their implementation in some places where it might be premature.

Q And as you — the President, yesterday, was talking about transitioning from the mass vaccination centers, largely in urban and suburban areas, and trying —

MS. PSAKI: Yeah.

Q — to really be more deliberate, proactive about getting the vaccine to people in outlying areas, rural areas.

Is there any concern about having enough vaccinators to reach people in those areas? And will this mostly be run through local pharmacies or is there going to be a similar effort to authorize

different people in sort of medical fields to be able to administer vaccines?

MS. PSAKI: Well, we did take that step some time ago to expand the type of individuals who are qualified to be vaccinators, because early on we recognized that it wasn't just about supply, it was also about locations — and obviously, as you alluded to, we've made some changes and adjustments — but also about vaccinators and ensuring that a larger group of individuals — dentists, veterinarians, others — could also be eligible to do the vaccine and get it into people's arms, because we want to ensure that in a range of communities across the country there's a range of options for people who can do exactly that.

So that's not a concern that we are tracking at this point in time — a lack of — because we did a lot of work preparing for those needs.

And I would say that, you know, there were some mass vaccination sites we opened even last week, but what we announced yesterday is a kind of a phased approach based on the phase we're in at this point in time, which is that we are recognizing the daily numbers will go down a bit because we're at such a high percentage rate, relative to where people thought we were at this point in the pandemic.

And we know it will be harder and harder to reach people and meet people where they are, hence the increase, as you suggested, in walk-in hours or the announcement of walk-in hours on mobile units, on partnerships with primary care physicians and doctors to make it even easier and more accessible for people to get the vaccine.

Q Just one more on tomorrow and the trip to Louisiana. So far, the President has mostly traveled to states that are, you know, competitive swing states. Louisiana is obviously a red state, but has been impacted by COVID.

MS. PSAKI: Except for Texas and Ohio.

Q Well, okay. But I mean, there's been a lot of travel to some of these states. Can you just talk a little bit about the takeaway that people should have when they see the President showing up, you know, in deep-red Louisiana tomorrow, and the issues that he wants to, sort of, draw attention to?

MS. PSAKI: Sure. Well, first, the President, when he was elected, knew from day one he was going to govern for all Americans and that was going to be his objective. And so, even if it's for people who didn't vote for him, for states who didn't vote for him, his focus is on delivering for

them.

So, tomorrow, he'll make two stops in Louisiana. His focus will be on talking about the American Jobs Plan and how that plan in a historic investment in infrastructure, rebuilding the type of bridges, roads in Louisiana that are long overdue to be upgraded could help not only people's travel and commutes, but also create jobs in these communities. And it's not about just delivering for people who voted for him or people who have blue checkmarks next to their name because they're Democrats. And that's part of what this message should shen- — this visit should send.

Go ahead, Hans.

Q I get that you, sort of, prefer the Moody's model over the Penn Wharton. I'm just curious if the White House is going to accept whatever CBO and JCT scores the President's proposals at?

MS. PSAKI: Well, I think our issue with the Penn Wharton Model was the data it was based on, and that it was off. And so we'll have to look at what the data that any future analysis is based on, and then we'll give an assessment.

Q Okay. So even official — you're not embracing whatever the official assessment will be from CBO and JCT?

MS. PSAKI: Well, Hans, there is no assessment at this point in time. Our assumption is that they would be abiding by accurate data; so we'll look forward to seeing those assessments.

Q And then when do you expect those assumptions and data to come in?

MS. PSAKI: I don't have a prediction of that.

Q Okay. Thank you.

MS. PSAKI: I suggest you ask them.

Go ahead, Alex.

Q Does President Biden agree with Governor Whitmer's decision on the oil and gas pipeline? She's citing, essentially, water-quality issues. It's really angered Canada. Does President Biden agree with that decision?

MS. PSAKI: I'd have to take a closer look at the pipeline. I mean, we have been evaluating on a case-by-case scenario — which — which pipeline are you talking about?

Q The Enbridge.

MS. PSAKI: The Enbridge one. We look at each pipeline through the prism of the impact on the environment and also the impact on the economy, and we make assessments. So I'd have to talk to our team if that assessment has been concluded or not.

Q Okay. And the President is going to be talking about implement — implementation later. What sort of oversight plans are being talked about, as far as the spending and making sure it's —

MS. PSAKI: For the restaurant program or just the programs in general?

Q In general. In general — Inspector Generals — I mean, can you give us an idea of what sort of oversight is being talked about?

MS. PSAKI: Well, first, the President came into this job having served as the person overseeing the implementation of the American Rescue and Recovery — of the ARRA — A-R-R-A — back in the early days of the Obama-Biden administration. He takes waste, fraud, and abuse incredibly seriously. And we have put in place changes and reforms to programs at SBA and other programs that have been implemented where we've seen incidents of that in the past.

It's also why he has somebody — Gene Sperling — overseeing the American Rescue Plan implementation to ensure there is coordination across government, that we are tracking where we see issues.

And certainly, he's somebody who welcomes oversight and wants to do everything we can to reduce any waste, fraud, and abuse in these programs.

Q And just finally, I wonder if the President or anyone else in the administration spoke with the Treasury Secretary yesterday, given some of her remarks that she then sought to clarify?

MS. PSAKI: Well, the Secretary, herself, addressed her remarks later in the afternoon. So I'm not aware of any calls yesterday. She will be here in the briefing room, and they'll have their regular economic briefing on Friday.

Go ahead, in the back.

Q So I want to talk about climate for a second. The President had said in his executive order in January that he would call for a Green Procurement Plan for the federal government.

MS. PSAKI: Mm-hmm.

Q And part of that was about buying electric cars. The deadline for that plan was April 27th. Do you know what the status of it is and why the delay?

MS. PSAKI: I don't have an update on the status. It is something, as you noted, he talked about early in the administration and he is absolutely committed to. But I'm happy to check with our team and see where our report on that lives.

Q And I also want to ask: Does the Biden administration have a timeline, at this point, for issuing pardons and commutations?

MS. PSAKI: I don't have any previewing of that to provide and probably won't from here.

Go ahead, in the back.

Q Yes. Is the Los Angeles mayor, Eric Garcetti, under active consideration to be the ambassador to India or any other country?

MS. PSAKI: I don't have any personnel announcements or assessments to make here from the podium. But, hopefully, we'll have some more formal announcements on ambassadors soon.

Q And the Tokyo Olympics are 12 weeks out.

MS. PSAKI: Mm-hmm.

Q At what point does the President need to make a decision about his attendance and —

MS. PSAKI: His attendance?

Q Yes. And what factors are delaying the announcement?

MS. PSAKI: Well, I think the President and his team assess any invitation as it comes in, but 12 weeks is some period of time. I don't have any updates or predictions on whether or not he'll travel or accept the invitation made to attend the Olympics.

Go ahead.

Q Thanks, Jen. Two questions. First, on the large sports arenas that are beginning to allow for fully vaccinated fans in special sections — both Citi Field and Yankee Stadium in New York have made those announcements, and I know there are some others. Does the administration think that that is a good approach for sports teams to take, and maybe other large event venues?

And are there any concerns about equity when it comes to access to facilities if — particularly, those that were built with some public money, in some cases, I'm sure — when it comes to people who may not have been able to get vaccinated yet?

MS. PSAKI: Well, first, everyone in the country is eligible to be vaccinated, and certainly at this point in time. So we are — and we, as we've noted here, have taken a range of steps to ensure we are meeting people where they are, getting these vaccine doses out to communities around the country.

In terms of an assessment of the safety of this approach by sports teams, I'd have to talk to our COVID team about that. And I think it's unlikely we're going to be weighing into every private sector decision about how they're moving forward once people are vaccinated, but I will check with them on that.

Q Okay. And then the other — the other question, if I can follow up on the — the debt limit question just a little bit.

MS. PSAKI: Sure.

Q Has there — does the — does the President have a position on whether or not the debt limit itself should exist at all, considering every — every, you know, couple of years we go through this question of: "What are the extraordinary measures?" And, "How much extra time do we have?" And we know, at the end of the day, that it's going to have to get raised or else we're going to have some sort of economic calamity.

Does the President have a view on the question, more broadly, of whether or not there even

should be a debt limit?

MS. PSAKI: Well, first, raising or suspending the debt ceiling doesn't authorize new spending; it merely allows Treasury to meet obligations that Congress has already approved. Right? It has been the case for many years and there have been bipartisan votes to support.

So, you know, the President does believe that Treasury should be able to meet its obligations and believes that Congress should move forward in a bipartisan manner, as they have historically in the past, including three times during the prior administration.

Go ahead, in the back.

Q Thanks. On the G7 trip, is there any advance on whether the President will meet with the Queen? And, separately, has the President or the First Lady been in contact recently with Prince Harry?

MS. PSAKI: I don't have any more trip details. Who among us wouldn't want to go see the Queen? But I don't have any details to preview at this point in time. I expect as we get closer to the trip, we'll have more specifics.

And I don't have any calls or engagements with Prince Harry or Meghan Markle to — to read out for you with the President or the First Lady.

Q Just one follow-up. Is there a timeline on the announcement for the British ambassador?

MS. PSAKI: A timeline?

Q Yeah.

MS. PSAKI: I don't have a timeline for that.

Q Any — any names or any — anyone under consideration?

MS. PSAKI: No names to float out there for you. Hopefully, we'll have some more ambassadors soon to announce.

Great.

Q When you say “soon,” will that be before or after he makes his decision on going to the Olympics?

MS. PSAKI: (Laughs.) I can’t order for you, Hans. There’s just so much excitement to stay tuned for around here. So, we’ll see.

Okay. Thanks everyone.

1:24 P.M. EDT

DEFENDANTS' EXHIBIT 148:

2019 WL 6715208 (D.O.J.)

Department of Justice (D.O.J.)

Attorney General (AG)

(NEWS RELEASE)

ATTORNEY GENERAL WILLIAM P. BARR DELIVERS REMARKS AT THE
NATIONAL ASSOCIATION OF ATTORNEYS GENERAL 2019 CAPITAL FORUM

December 10, 2019

Remarks as Prepared for Delivery

Good afternoon. Thank you General Landry for that kind introduction, and thank you to the National Association of Attorneys General (NAAG) for inviting me to join you today. It is an honor and privilege to be here with my fellow attorneys general.

Through the Executive Working Group and in various operations, we are working together on several important law enforcement priorities. Elder Justice is a personal priority for me, and I know the State AGs have been leading the charge for many years. Derrick Schmidt's Presidential initiative highlighted the impact of this important issue. Each year, over three billion dollars are stolen or defrauded from millions of America's elderly through a variety of malicious scams. The State AGs are on the front line in this fight to protect the elderly from being exploited, and I pledge the Department's full support in that effort.

Similarly, human trafficking is an extremely important law enforcement issue for both the DOJ and the States AGs. Attorneys General Paxton, Healey, Bacerra, Reyes and many others have been leaders in this vital effort. We worked together to take down backpage.com, and we continue to engage our state partners through our Human Trafficking Prosecutorial Unit. We look forward to continuing that work with you to make more progress in the year ahead.

In addition to these important priorities, another topic that involves almost every AG in this room and one that also benefits from close federal-state cooperation is the review into market-leading online platforms.

I. Benefits of Broad State AG Support on Review of Market-Leading Online Platforms

In DC, it's hard to find many things that everyone agrees on. One thing that has found wide and bi-partisan support, however, is the government taking a closer look at the leading online platforms and the competitiveness of digital markets.

Online platforms play an important role in our economy and in Americans' daily lives, often serving as gateways for how we access goods, services, information and even each other.

A few digital platforms in particular have enjoyed significant growth over the past decade. Consumers now depend on these platforms every day. Their size and pervasiveness have led to public concerns about the competitive health of these digital markets.

We've heard widespread concerns from consumers, businesses and entrepreneurs, including about stagnated innovation, high prices, lack of choice, privacy, transparency, and public safety. In response, DOJ initiated a review into market-leading online platforms, which we announced publicly last July.

Concerns about online platforms have come from a wide variety of stakeholders, across the political spectrum. Indeed, almost every State AG is now participating in publicly announced antitrust investigations of Google and Facebook. I've had the benefit of meeting with representatives of these groups at the Department, and believe we have a good cooperative relationship in these efforts.

This is not the first time that the Department of Justice has cooperated with a bi-partisan coalition of State AGs on an antitrust matter involving a digital platform.

When the Department of Justice litigated a case against Microsoft roughly 20 years ago for antitrust violations, it was joined by a coalition of 20 state attorneys general and the District of Columbia. There are still those in the Department and State AG community, including my friend Tom Miller, who were closely involved and remember it well.

Today, the State AG coalitions investigating Google and Facebook are even bigger than in *Microsoft*, including almost every state and federal territory. I think this demonstrates the importance of these issues to Americans across the country, regardless of location or political persuasion.

II. Benefits of a Broad, Holistic Perspective

The benefits of a broad approach to online platforms go beyond building a federal-state partnership. A broader, holistic perspective is also important as we consider substantive issues raised by the digital economy, both within and outside of the arena of antitrust.

Let me start with antitrust. Antitrust is a core focus of the Department's review into market-leading platforms because, ultimately, fair competition can cure many of the ills we see. In a functioning free market, consumers can demand alternatives that better address their preferences, including for greater privacy, more transparency, or increased safety. For consumer choice and the free market to work, however, firms have to be playing by the established rules of competition. That's where antitrust enforcement steps in.

Many online platforms are not only big, but also offer a wide breadth of products and services. Antitrust enforcers therefore must take an equally broad view of these platforms' offerings, and the relationships between different markets, products, and business practices.

Let me touch on a few examples of where a broader perspective is useful in an antitrust analysis.

First, a broader perspective requires understanding the characteristics of the market. This includes looking at whether there are high barriers to entry that prevent or deter new competitors. For example, digital platform markets are often characterized by economies of scale and scope, including direct and indirect network effects.

Take, for example, direct network effects in social media. The more users on the same social media platform, the more valuable that platform is overall. There are benefits to consumers from being on the same network as their friends and family. At the same time, the existence of such network effects can make it harder for a new platform to attract users.

This positive feedback loop is also inherent in platforms that rely on data and machine-learning. For example, generally speaking, the more data a search engine has, the better its algorithms for search results can be. The better the algorithm, the more users it can attract, and with them comes even more data. And the cycle starts anew.

Digital platforms can also have indirect network effects, meaning the more users on one side of the platform increases the value to users on the other side of the platform.

In *Microsoft*, for example, there were indirect network effects that created what the court described as an “applications barrier to entry.” The more consumers that used the Microsoft operating system, the more attractive the platform was to application developers. Conversely, the more applications that were on the Microsoft operating system, the more attractive the platform was for users. These indirect network effects created a barrier to entry that helped protect Microsoft's monopoly.

Network effects are not inherently problematic. However, where strong network effects create a significant barrier to entry, it can lead to increased market power, which in turn can be used in anticompetitive ways.

Given these dynamics, antitrust enforcers must be particularly vigilant to police for agreements and conduct that harm the competitive process.

Similarly, market power is not itself wrongful. As I've said before, big is not necessarily bad. Healthy competition creates winners and losers, and the prospect of winning (and the profits that come with it) can drive innovation in the first place. Success that comes from creating a better, more innovative product should be applauded. The danger, however, is that a monopolist (even one who earned that status lawfully) can be tempted to use their power to engage in anticompetitive conduct to preserve their dominant position.

Moreover, the existence of market power can change the competitive effects of a business practice. Conduct that may be procompetitive for a new entrant can become anticompetitive if undertaken by the incumbent 800 pound gorilla.

For example, exclusivity agreements by a new entrant can increase competition by enabling a competitor to attract users with unique offerings, even in markets with strong network effects. At the same time, exclusive dealing by a monopolist could have the opposite effect by depriving rivals of the inputs or scale necessary to compete.

Bundling, tying, predatory pricing, and certain refusals to deal are other examples of conduct that can become problematic when undertaken by a firm with market or monopoly power.

As digital firms transition from being the disruptive new entrant into an established market leader, they should pay attention to the impact of their business practices. So too should the antitrust enforcers.

Second, in addition to understanding the dynamics within a market, like barriers to entry and market power, we also need to look at relationships between markets. This is especially important because today's digital platforms frequently operate across multiple areas.

A dominant firm may seek to leverage its monopoly power in one market to gain an unfair advantage in another. In the *Microsoft* case, for example, a key concern was that Microsoft was abusing its dominant position in operating systems to foreclose competition in browsers.

The relationships between markets can be even more complex in the digital age, with the emergence of new business models and an increasingly important role of data. Law enforcers need to better understand how consumer data is collected, used, and shared within a firm and with third parties. Such antitrust inquiries generally require a broader perspective and deeper understanding of how each of these markets function.

Third, taking a broader perspective is particularly important in the context of “free” online services. Digital platforms are not charities. When they offer services to consumers for “free,” that just means they are making money somewhere else, either through a different product, from different consumers, or at a different point in time.

The increasing prevalence and complexity of “free” digital services may require a broader perspective.

For example, antitrust enforcers may need to look beyond the free service to better understand a firm's monetization strategy and incentives. Enforcers also may need to look more closely at non-price effects. Fortunately, the long-standing consumer welfare standard enables us to analyze non-price effects on competition, including on quality, innovation, and consumer choice.

A broader perspective also requires looking beyond antitrust. As we listen to complaints from the public, industry, and experts, it has become clear that not every problem related to online platforms comes within the reach of antitrust law.

Some have therefore proposed expanding the antitrust laws to reach other non-economic harms. Drastically re-inventing the antitrust laws, however, is neither easy nor advisable. The Sherman Act has been around for over a century and has proved flexible enough to adapt to a wide variety of industries, including digital platforms. We are open to considering new tools and targeted modifications, but a wholesale departure from the antitrust laws' focus on competition is unwarranted.

While we should not distort the antitrust laws, the Department of Justice also cannot ignore real harms to the American people. Where there are non-competition harms, the Department will consider whether there are other tools - including other legal or policy frameworks - that can help. We are thinking critically about how the Department, and our state and federal partners, can address other topics related to online platforms, such as privacy, transparency, consumer fraud, child exploitation, or public safety.

One example of a non-antitrust issue related to online platforms is Section 230 of the Communications Decency Act. Generally speaking, Section 230 provides immunity to interactive computer services for third-party content on their platforms.

As this group well knows, there is currently a robust public debate over Section 230. The NAAG sent a letter to Congress last May, proposing an amendment that would carve out U.S. state and territorial criminal law from the current scope of Section 230 immunity. We, too, are studying Section 230 and its scope.

The CDA was passed in 1996 in response to concerns about protecting children from sexually explicit content on the internet. Section 230 was enacted primarily for two purposes.

The primary purpose of the amendment was to encourage platforms to self-regulate by granting immunity for blocking or filtering offensive material. In particular, the amendment aimed to overrule a 1995 state court decision that treated an online message board as a publisher of third-party content, and thus liable for defamation, because the service restricted access to some, but not other, objectionable material.

Another purpose was to encourage the growth of online forums by immunizing platforms against liability for third party speech. Section 230 was passed at a time where the internet was relatively new, and Congress wanted to protect the growth of online services and the ability for the internet to offer "a forum for true diversity of political discourse."

Section 230 has been interpreted quite broadly by the courts. Today, many are concerned that Section 230 immunity has been extended far beyond what Congress originally intended. Ironically, Section 230 has enabled platforms to absolve themselves completely of responsibility for policing their platforms, while blocking or removing third-party speech - including political speech - selectively, and with impunity.

Some also question whether such a broad immunity is still necessary to protect online companies. Indeed, ten years ago, a Ninth Circuit opinion denying Section 230 immunity in part remarked: "The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses." *Fair Housing Council of San Fernando Valley v. Roommates.com LLC*, 521 F.3d 1157, 1164 n. 15 (9th Cir. 2008). In other words, the opinion stated: "the Internet has outgrown its swaddling clothes and no longer needs to be so gently coddled." *Id.* at 1175, n. 39.

The staggering breadth of Section 230 immunity, as construed by the courts, is evident in a recent Second Circuit opinion involving the Anti-Terrorism Act. See *Force v. Facebook, Inc.*, 934 F.3d 53 (2nd Cir. 2019). There, the court held that Facebook was immune under Section 230 for allegedly matching and facilitating communications between members of the terrorist group Hamas. The court denied plaintiff's argument that Facebook's algorithms and friend-matching service rendered it a "non-publisher" outside the scope of Section 230. *Id.* at 66.

Chief Judge Katzmann dissented in part, criticizing the virtually limitless scope of Section 230 immunity imposed by some courts. He argued that providing immunity for the steps Facebook took to connect alleged terrorists through algorithm and friend suggestions was far removed from the original purpose of the CDA to protect children against obscene material online. He called for Congress to revisit the CDA to "better calibrate the circumstances where such immunization is appropriate and inappropriate in light of congressional purposes." *Id.* at 77.

Chief Judge Katzmann is not alone in his calls for reform. Section 230 has garnered significant attention from experts, consumer groups, and legislators. Within DOJ, we also have started thinking critically this issue.

The purpose of Section 230 was to protect the "good Samaritan" interactive computer service that takes affirmative steps to police its own platform for unlawful or harmful content. Granting broad immunity to platforms that take no efforts to mitigate unlawful behavior or, worse, that purposefully blind themselves -- and law enforcers -- to illegal conduct occurring on, or facilitated by, the online spaces they create, is not consistent with that purpose.

We want to engage further with experts, industry, and other government actors, including the NAAG, through informal discussions as well as a public workshop.

III. Coordination is Key

As we look at Section 230, antitrust, and other issues raised by the online platforms, it is important to take a coordinated approach.

The issues raised by online platforms are interrelated, and we sometimes must weigh competing interests in forming positions related to the digital economy.

Privacy is a good example. Overbroad and overly burdensome privacy legislation could inhibit competition by entrenching monopolists with the resources to comply, while thwarting newer entrants who do not have those resources.

A single-minded focus on privacy, above all other values, also can impose significant costs, including costs to public safety. I have, for example, spoken before about the dangers of warrant-proof encryption. I won't repeat myself here, but would simply reiterate that technological innovations that purport to protect privacy at all costs - while impeding sworn law enforcers' ability to go after violent criminals, child predators, human traffickers, and terrorists, even once the enforcers satisfied the rigorous privacy protections built into the Fourth Amendment -- may not be worth the trade-off.

High level coordination in our review of market-leading online platforms also helps avoid imposing conflicting obligations or inconsistent policy positions. This requires coordination both within and outside DOJ.

While we have some of the best and brightest at the DOJ's Antitrust Division and across the Department working on these issues, we benefit from the perspective and support of our State AG, federal, and international partners. We are also welcoming consumers, businesses, experts, and others to talk and work with us to address the challenges of the digital age.

The technology industry in America has brought great innovations to consumers in the US and around the world. We must continue to encourage and incentivize innovation and economic growth. This means not unfairly punishing innovators that have earned their success on the merits. But it also means making sure markets are competitive and open to the next wave of technological change.

As law enforcers, we also must keep up with technological advancements to best protect our citizens. This is why we have made the review of market-leading online platforms a top priority of the Department.

The State AG community plays a very important role in this endeavor. On behalf of DOJ, I thank you all for your valuable partnership and look forward to our continued work together on this and many other initiatives.

2019 WL 6715208 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 149:

2018 WL 3471764 (D.O.J.)

Department of Justice (D.O.J.)

Deputy Attorney General (DAG)

(NEWS RELEASE)

DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN
DELIVERS REMARKS AT THE ASPEN SECURITY FORUM

July 19, 2018

Remarks as prepared for delivery

It is a privilege to join you this afternoon at one of the world's premier security conferences.

We meet at a fraught moment. For too long, along with other nations, we enjoyed the extraordinary benefits of modern technology without adequately preparing for its considerable risks. Director of National Intelligence Dan Coats elevated the alarm last week, when he stated that “the digital infrastructure that serves this country is literally under attack.” That is one of the rare instances when the word literally is used literally.

Our adversaries are developing cyber tools not only to steal our secrets and mislead our citizens, but also to disable our infrastructure by gaining control of computer networks.

Every day, malicious cyber actors infiltrate computers and accounts of individual citizens, businesses, the military, and all levels of government. Director Coats revealed that our adversaries “target[] government and businesses in the energy, nuclear, water, aviation and critical manufacturing sectors.” They cause billions of dollars in losses, preposition cyber tools they could use for future attacks, and try to degrade our political system. So combating cybercrime and cyber-enabled threats to national security is a top priority of the Department of Justice.

Attorney General Jeff Sessions established a Cyber-Digital Task Force in February to consider two questions: What are we doing now to address cyber threats? And how can we do better?

Today, the Department of Justice is releasing a report that responds to the first question, providing a detailed assessment of the cyber threats confronting America and the Department's efforts to combat them.

The Task Force report addresses a wide range of issues, including how to define the multi-faceted challenges of cyber-enabled crime; develop strategies to detect, deter and disrupt threats; inform victims and the public about dangers; and maintain a skilled workforce.

The report describes six categories of cyber threats, and explains how the Department of Justice is working to combat them.

One serious type of threat involves direct damage to computer systems, such as Distributed Denial of Service attacks and ransomware schemes.

Another category is data theft, which includes stealing personally identifiable information and intellectual property.

The third category encompasses cyber-enabled fraud schemes.

A fourth category includes threats to personal privacy, such as sextortion and other forms of blackmail and harassment.

Attacks on critical infrastructure constitute the fifth category. They include infiltrating energy systems, transportation systems, and telecommunications networks.

Each of those complex and evolving threats is serious, and the report details the important work that the Department of Justice is doing to protect America from them.

I plan to focus today on a sixth category of cyber-enabled threats: malign foreign influence operations, described in chapter one of the task force report.

The term “malign foreign influence operations” refers to actions undertaken by a foreign government, often covertly, to influence people's opinions and advance the foreign nation's strategic objectives. The goals frequently include creating and exacerbating social divisions and undermining confidence in democratic institutions.

Influence operations are a form of information warfare. Covert propaganda and disinformation are among the primary weapons.

The Russian effort to influence the 2016 presidential election is just one tree in a growing forest. Focusing merely on a single election misses the point. As Director Coats made clear, “these actions are persistent, they are pervasive, and they are meant to undermine America's democracy on a daily basis, regardless of whether it is election time or not.”

Russian intelligence officers did not stumble onto the ideas of hacking American computers and posting misleading messages because they had a free afternoon. It is what they do every day.

This is not a new phenomenon. Throughout the twentieth century, the Soviet Union used malign influence operations against the United States and many other countries. In 1963, for example, the KGB paid an American to distribute a book claiming that the FBI and the CIA assassinated President Kennedy.

In 1980, the KGB fabricated and distributed a fake document claiming that there was a National Security Council strategy to prevent black political activists from working with African leaders.

During the Reagan Administration, the KGB spread fake stories that the Pentagon developed the AIDS virus as part of a biological weapons research program.

As Jonathan Swift wrote in 1710, “Falsehood flies, and the Truth comes limping after it.”

The Reagan Administration confronted the problem head on. It established an interagency committee called “the Active Measures Working Group” to counter Soviet disinformation. The group exposed Soviet forgeries and other propaganda.

Modern technology vastly expands the speed and effectiveness of disinformation campaigns. The Internet and social media platforms allow foreign agents to spread misleading political messages while masquerading as Americans.

Homeland Security Secretary Kirstjen Nielsen explained last weekend that our adversaries “us[e] social media, sympathetic spokespeople and other fronts to sow discord and divisiveness amongst the American people.”

Elections provide an attractive opportunity for foreign influence campaigns to undermine our political processes. According to the intelligence community assessment, foreign interference in the 2016 election “demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.”

The Department's Cyber-Digital Task Force report contributes to our understanding by identifying five different types of malign foreign influence operations that target our political processes.

First, malicious cyber actors can target election infrastructure by trying to hack voter registration databases and vote-tallying systems. In 2016, foreign cyber intruders targeted election-related networks in as many as 21 states. There is no evidence that any foreign government ever succeeded in changing votes, but the risk is real. Moreover, even the possibility that manipulation may occur can cause citizens to question the integrity of elections.

Second, cyber operations can target political organizations, campaigns, and public officials. Foreign actors can steal private information through hacking, then publish it online to damage a candidate, campaign, or political party. They can even alter that stolen information to promote their desired narrative.

Russia's intelligence services conducted cyber operations against both major U.S. political parties in 2016, and the recent indictment of Russian intelligence officers alleges a systematic effort to leak stolen campaign information.

The third category of malign influence operations affecting elections involves offers to assist political campaigns or public officials by agents who conceal their connection to a foreign government. Such operations may entail financial and logistical support to unwitting Americans.

Fourth, adversaries covertly use disinformation and other propaganda to influence American public opinion. Foreign trolls spread false stories online about candidates and issues, amplify divisive political messages to make them appear more pervasive and credible, and try to pit groups against each other. They may also try to affect voter behavior by triggering protests or depressing voter turnout.

Finally, foreign governments use overt influence efforts, such as government-controlled media outlets and paid lobbyists. Those tactics may be employed lawfully if the foreign agents comply with registration requirements. But people should be aware when lobbyists or media outlets are working for a foreign government so they can evaluate the source's credibility. Particularly when respected figures argue in favor of foreign interests, it may matter to know that they are taking guidance from a foreign nation.

The election-interference charges filed in February demonstrate how easily human “trolls” distribute propaganda and disinformation. A Russian man recently admitted to a reporter that he worked with the trolls, in a separate department creating fake news for his own country. He “felt like a character in the book '1984' by George Orwell - a place where you have to write that white is black and black is white.... [Y]ou were in some kind of factory that turned lying ... into an industrial assembly line. The volumes were colossal - there were huge numbers of people, 300 to 400, and they were all writing absolute untruths.”

When the man took a test for a promotion to the department working to fool Americans, he explained, “The main thing was showing that you are able to ... represent yourself as an American.”

The former troll believes that Russian audiences pay no attention to fake internet comments. But he has a different opinion about Americans. He thinks that we can be deceived, because Americans “aren't used to this kind of trickery.”

That remark is sort of a compliment. In repressive regimes, people always assume that the government controls media outlets. We live in a country that allows free speech, so people are accustomed to taking it seriously when other citizens express their opinions. But not everyone realizes that information posted on the Internet may not even come from citizens.

Moreover, Internet comments may not even come from human beings. Automated bots magnify the impact of propaganda. Using software to mimic actions by human users, bots can circulate messages automatically, creating the appearance that thousands

of people are reading and forwarding information. Together, bots and networks of paid trolls operating multiple accounts allow foreign agents to quickly spread disinformation and create the false impression that it is widely accepted.

The United States is not alone in confronting malign foreign influence. Russia reportedly conducted a hack-and-release campaign against President Macron during last year's French elections, and instituted similar operations against political candidates in other European democracies. Other foreign nations also engage in malign influence activities.

So what can we do to defend our values in the face of foreign efforts to influence elections, weaken the social fabric, and turn Americans against each other? Like terrorism and other national security threats, the malign foreign influence threat requires a unified, strategic approach across all government agencies. The Departments of Justice, Homeland Security, State, Defense, Treasury, Intelligence agencies, and others play important roles.

Other sectors of society also need to do their part. State and local governments must secure their election infrastructure. Technology companies need to prevent misuse of their platforms. Public officials, campaigns, and other potential victims need to study the threats and protect themselves and their networks. And citizens need to understand the playing field.

The Department of Justice investigates and prosecutes malign foreign influence activity that violates federal criminal law. Some critics argue against prosecuting people who live in foreign nations that are unlikely to extradite their citizens. That is a shortsighted view.

For one thing, the defendants may someday face trial, if there is a change in their government or if they visit any nation that cooperates with America in enforcing the rule of law. Modern forms of travel and communication readily allow criminals to cross national boundaries. Do not underestimate the long arm of American law - or the persistence of American law enforcement. People who thought they were safely under the protection of foreign governments when they committed crimes against America sometimes later find themselves in federal prisons.

Second, public indictments achieve specific deterrence by impeding the defendants from traveling to rule-of-law nations and raising the risk they will be held accountable for future cybercrime. Wanted criminals are less attractive co-conspirators.

Third, demonstrating our ability to detect and publicly charge hackers will deter some others from engaging in similar conduct.

Fourth, federal indictments are taken seriously by the public and the international community, where respect for our criminal justice system - including an understanding of the presumption of innocence and the standard of proof beyond a reasonable doubt - means that our willingness to present evidence to a grand jury and ultimately at trial elicits a high degree of confidence in our allegations.

Fifth, victims deserve vindication, particularly when they are harmed by criminal acts that would be prosecuted if the perpetrator were located in the United States.

Sixth, federal criminal investigations support other penalties for malign foreign influence operations. For example, the Department of the Treasury can impose financial sanctions on defendants based on evidence exposed in indictments. Voters in foreign democracies, and influential citizens in autocratic regimes, can consider the allegations in making their own decisions about national leadership and foreign alliances.

The Department of the Treasury imposed sanctions on the individuals and entities identified in the February election-interference indictment, along with others engaged in malign activities. Nineteen individuals and five entities are subject to sanctions that freeze assets under American jurisdiction. Even if they are never brought to court, they will face consequences.

The sanctions forbid those individuals and entities from engaging in transactions with Americans and using the American financial system. The Administration followed up with similar financial sanctions for a broader range of malign activities against seven oligarchs, 12 companies, 17 Russian government officials, and two other entities.

Prosecutions are one useful tool to help deter modern criminals who remain beyond our shores. The same approach applies outside the context of crimes committed to influence elections. That is why our government regularly files charges against criminals who hide overseas, such as Iranian government hackers who broke into computer networks of a dam; Iranian hackers who infiltrated American universities, businesses and government agencies for the Islamic Revolutionary Guard Corps; an Iranian hacker who infiltrated and extorted a television network; Chinese government hackers who committed economic espionage; and Russian intelligence officers who stole data from an email service provider.

Intelligence assessments and criminal indictments are based on evidence. They do not reflect mere guesses. Intelligence assessments include analytical judgments based on classified information that cannot be disclosed because the evidence is from sources - people who will be unable to help in the future if they are identified and might be harmed in retaliation for helping America - and methods - techniques that would be worthless if our adversaries knew how we obtained the evidence. Indictments are based on credible evidence that the government must be prepared to introduce in court if necessary.

Some people may believe they can operate anonymously on the Internet, but cybercrime generally creates electronic trails that lead to the perpetrators.

Gathering intelligence about adversaries who threaten our way of life is a noble task. Outside the Department of Justice headquarters stands a statue of Nathan Hale. Hale was executed immediately, without a trial, after he was caught gathering intelligence for America during the Revolutionary War. His final words are recorded as follows: "I am so satisfied with the cause in which I have engaged, that my only regret is that I have but one life to offer in its service."

The days when foreign criminals could cause harm inside America from remote locations without fear of consequences are past. If hostile governments choose to give sanctuary to perpetrators of malicious cybercrimes after we identify them, those governments will need to take responsibility for the crimes, and individual perpetrators will need to consider the personal cost.

But criminal prosecutions and financial sanctions are not a complete solution. We need to take other steps to prevent malicious behavior.

To protect elections, the first priority is to harden our infrastructure. State governments run American elections and are responsible for maintaining cybersecurity, but they need federal help. The Department of Homeland Security takes the lead in helping to protect voting infrastructure, and the FBI leads federal investigations of intrusions.

The FBI works closely with DHS to inform election administrators about threats. DHS and the FBI provide briefings to election officials from all fifty states about our foreign adversaries' intentions and capabilities.

We also seek to protect political organizations, campaigns, candidates, and public officials. The FBI alerts potential victims about malicious cyber activities and helps them respond to intrusions. It shares detailed information about threats and vulnerabilities.

To combat covert foreign influence on public policy, we enforce federal laws that require foreign agents to register with the U.S. government. Those laws prohibit foreign nationals from tricking unwitting Americans while concealing that they are following orders from foreign government handlers. The Department of Justice is stepping up enforcement of the Foreign Agents Registration Act and related laws, and providing defensive counterintelligence briefings to local, state, and federal leaders and candidates.

Public attribution of foreign influence operations can help to counter and mitigate the harm caused by foreign government-sponsored disinformation. When people are aware of the true sponsor, they can make better-informed decisions.

We also help technology companies to counter covert foreign influence efforts. The FBI works with partners in the Intelligence Community to identify foreign agents as they establish their digital infrastructure and develop their online presence. The FBI helps technology companies disrupt foreign influence operations, by identifying foreign agents' activities so companies may consider the voluntary removal of accounts and content that violate terms of service and deceive customers.

Technology companies bear primary responsibility for securing their products, platforms, and services from misuse. Many are now taking greater responsibility for self-policing, including by removing fake accounts. We encourage them to make it a priority to combat efforts to use their facilities for illegal schemes.

Even as we enhance our efforts to combat existing forms of malign influence, the danger continues to grow. Advancing technology may enable adversaries to create propaganda in new and unforeseen ways. Our government must continue to identify and counter them.

Exposing schemes to the public is an important way to neutralize them. The American people have a right to know if foreign governments are targeting them with propaganda.

In some cases, our ability to expose foreign influence operations may be limited by our obligation to protect intelligence sources and methods, and defend the integrity of investigations.

Moreover, we should not publicly attribute activity to a source unless we possess high confidence that foreign agents are responsible. We also do not want to unduly amplify an adversary's messages, or impose additional harm on victims.

In all cases, partisan political considerations must play no role in our efforts. We cannot seek to benefit or harm any lawful group, individual or organization. Our government does not take any official position on what people should believe or how they should vote, but it can and should protect them from fraud and deception perpetrated by foreign agents.

Unfettered speech about political issues lies at the heart of our Constitution. It is not the government's job to determine whether political opinions are right or wrong.

But that does not leave the government powerless to address the national security danger when a foreign government engages in covert information warfare. The First Amendment does not preclude us from publicly identifying and countering foreign government-sponsored propaganda.

It is not always easy to balance the many competing concerns in deciding whether, when, and how the government should disclose information about deceptive foreign activities relevant to elections. The challenge calls for the application of neutral principles.

The Cyber-Digital Task Force Report identifies factors the Department of Justice should consider in determining whether to disclose foreign influence operations. The policy reflects an effort to articulate neutral principles so that when the issue the government confronted in 2016 arises again - as it surely will - there will be a framework to address it.

Meanwhile, the FBI's operational Foreign Influence Task Force coordinates investigations of foreign influence campaigns. That task force integrates the FBI's cyber, counterintelligence, counterterrorism, and criminal law enforcement resources to ensure that we understand threats and respond appropriately. The FBI task force works with other federal agencies, state and local authorities, international partners, and the private sector.

Before I conclude, I want to emphasize that covert propaganda disseminated by foreign adversaries is fundamentally different from domestic partisan wrangling. As Senator Margaret Chase Smith proclaimed in her 1950 declaration of conscience, we must address foreign national security threats “patriotically as Americans,” and not “politically as Republicans and Democrats.”

President Reagan's Under Secretary of State, Lawrence Eagleburger, wrote about Soviet active measures in 1983. He said that “it is as unwise to ignore the threat as it is to become obsessed with the myth of a super Soviet conspiracy manipulating our essential political processes.” He maintained that free societies must expose disinformation on a “persistent and continuing” basis.

Over the past year, Congress passed three statutes encouraging the Executive Branch to investigate, expose, and counter malign foreign influence operations. Publicly exposing such activities has long been a feature of U.S. law. The Foreign Agents Registration Act, which Congress enacted in 1938 to deter Nazi propagandists, mandates that the American public know when foreign governments seek to influence them.

Knowledge is power. In 1910, Theodore Roosevelt delivered a timeless speech about the duties of citizenship. It is best known for the remark that “it is not the critic who counts.” But Roosevelt's most insightful observation is that the success or failure of a republic depends on the character of the average citizen. It is up to individual citizens to consider the source and evaluate the credibility of information when they decide what to believe.

Heated debates and passionate disagreements about public policy and political leadership are essential to democracy. We resolve those disagreements at the ballot box, and then we keep moving forward to future elections that reflect the will of citizens. Foreign governments should not be secret participants, covertly spreading propaganda and fanning the flames of division.

The government plays a central role in combating malign foreign influence and other cyber threats. The Attorney General's Cyber-Digital Task Force report demonstrates that the Department of Justice is doing its part to faithfully execute our oath to preserve, protect, and defend America.

I regret that my time today is insufficient to describe the report in greater detail. It is available on the Department of Justice website. I hope you read it and find it a useful contribution to public discussion about one of the most momentous issues of our time.

In brief, the report explains that we must continually adapt criminal justice and intelligence tools to combat hackers and other cybercriminals. Traditional criminal justice is most often characterized by police chasing criminals and eyewitnesses pointing out perpetrators in courtrooms. Cybercrime requires additional tools and techniques.

We limit cybercrime damage by seizing or disabling servers, domain names, and other infrastructure that criminals use to facilitate attacks. We shut down the dark markets where criminals buy and sell stolen information. We restore control of compromised computers. We share information gathered during our investigations to help potential victims protect themselves. We seek restitution for victims. We pursue attribution and accountability for perpetrators. And we expose governments that defraud and deceive our citizens.

The Task Force report is just one aspect of our efforts. It is a detailed snapshot of how the Department of Justice assesses and addresses current cyber threats. The work continues, and not just within our Department.

Our government is doing more now than ever to combat malign foreign influence and other cyber threats. Trump Administration agency appointees and White House officials work with career professionals every day to prevent cybercrime and protect elections.

Our adversaries will never relent in their efforts to undermine America, so we must remain eternally vigilant in the defense of liberty, and the pursuit of justice. And we must approach each new threat united in our commitment to the principle reflected in the motto adopted at the founding of our Republic: e pluribus unum.

Thank you.

2018 WL 3471764 (D.O.J.)

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 150:

NewsRoom

7/3/20 WashingtonPost.com (Pg. Unavail. Online)
2020 WLNR 18548780

WashingtonPost.com
Copyright (c) 2020 The Washington Post

July 3, 2020

Section: /technology

Facebook is working to persuade advertisers to abandon their boycott. So far, they aren't impressed.

Elizabeth Dwoskin; Taylor Telford

Facebook has spent the past few days in round-the-clock conversations with advertisers, trying to persuade them to come back to the platform with the promise of modest changes to address concerns that the social network profits from hate and outrage.

But advertisers and the agencies they work with say they are still negotiating. And they say they are so far unimpressed with promises to better police hate speech, including labeling some politicians' posts when they break the company's policies. On Tuesday, when the civil rights groups that organized the efforts expect to sit down with chief executive Mark Zuckerberg, they plan to push for a rash of changes, including adding a C-suite-level executive dedicated to ensuring that the company's policies don't contribute to racism and radicalization.

More than 750 companies including Coca-Cola, Hershey and Unilever have already temporarily paused their advertising on Facebook and its subsidiary Instagram. More companies have joined the movement every day, with recent additions including Walgreens, Best Buy, Ford and Adidas. More than 200 advertisers joined in the past 24 hours.

Kerri Pollard, senior vice president of the membership platform Patreon — which is pulling all of its ads from Facebook and Instagram — said that the recent string of concessions still did little to address the company's core concern: Zuckerberg's characterization of free speech. The Facebook CEO has said he believes that social platforms should not fact-check politicians.

"Until he softens that, which would affect that entire business internally and externally, we're not going to feel comfortable returning to the platform," Pollard said. Patreon in 2018 booted far-right personalities off its platform in response to criticism.

But fact-checking politicians could have wide-ranging consequences, too. Facebook's business model depends on engagement: The more time people spend viewing content on the platform, and the more they click and interact with others, the more they are exposed to advertising in Facebook's scrolling news feed. Critics have argued that divisive and emotional content spreads more rapidly, particularly in like-minded private Facebook groups. That outrage is built into Facebook's ability to profit.

The boycott is the largest flare-up in a long-simmering battle between advertisers and social platforms over who gets to control what content the ads pop up next to. The campaign, which was triggered by Facebook allowing content that organizers said could incite violence against protesters, represents the most substantive effort to date to sanction the social network, which commands the second-largest share of the U.S. digital ad market behind Google.

Facebook spokeswoman Ruchika Budhraj said in a statement that it invests billions every year to keep users safe and works with outside experts to update its policies.

"We've opened ourselves up to a civil rights audit, and we have banned 250 white supremacist organizations from Facebook and Instagram," she said. "We know we have more work to do, and we'll continue to work with civil rights groups, [the Global Alliance for Responsible Media], and other experts to develop even more tools, technology and policies to continue this fight."

Still, the initiative probably won't affect Facebook's bottom line. The company has 8 million advertisers, which generated almost all of its approximately \$70 billion in ad revenue last year. Most are small businesses.

"Given Facebook's colossal scandals and rare repercussions to revenue, the advertisers' boycott is a body blow that will decimate Facebook's top line. I expect to see a revenue bleed out of more than \$7.5 billion in 2020," said Eric Schiffer, chairman and chief executive of the Patriarch Organization and Reputation Management Consultants.

Zuckerberg appears to have to dug in. He told employees last week at a company meeting that he wasn't going to "change our policies or our approach on anything because of a threat to a small percent of our revenue, or to any percent of our revenue," according to the Information.

Facebook has been meeting and talking with advertisers "almost every minute of every day," said a senior executive of a major ad agency who, like others for this story, spoke on the condition of anonymity because the company works closely with Facebook. Another ad industry executive who participated in meetings with Facebook said she came out disappointed.

The company is "slow and blame-sharing, acting like they are just the platform and society itself is full of bad actors," she said. She added that it is also blaming rivals YouTube and Twitter for their own practices over hate speech.

The reckoning goes beyond Facebook. A recent survey of nearly 60 companies by the World Federation of Advertisers found that about a third were likely to halt ad spending across social media due to hate speech, while 40 percent were considering doing so. Companies including Coca-Cola, Verizon and Unilever say they are reconsidering their ad spending not just on Facebook, but on all social media platforms.

Some skeptics say it's convenient timing for the advertisers, many of which are already cutting their marketing budgets amid a downturn in consumer spending.

The campaign against Facebook first emerged amid a national conversation on race sparked by the killing of George Floyd, an unarmed black man in Minnesota. Organizers said that Facebook's platform in particular was providing a forum for violent militia groups with plans to attack protesters. Some self-described members of those groups have been arrested in recent weeks for carrying weapons to protests and for allegedly planning to commit violent acts.

"It was the killing of George Floyd that told us that we needed to move," said Jonathan Greenblatt, chief executive of the Anti-Defamation League, one of the civil rights groups behind the campaign.

"It was an obvious moment to say, you can't talk about race in your news release but not stand for racial justice in your product," he said, referring to social media companies publicly sharing support for the Black Lives Matter movement.

Outdoor apparel company North Face was the first to join, followed by industry peers Patagonia and R.E.I. Those companies are known for taking stances on social issues.

"The stakes are too high to sit back and let the company continue to be complicit in spreading disinformation and fomenting fear and hatred," Patagonia tweeted on June 21 as it joined the #StopHateForProfit campaign.

The campaign's demands are broad and aim to address a host of grievances, including the removal of Facebook groups dedicated to white supremacy, militia movements, Holocaust denialism, vaccine misinformation and climate denialism. The campaign also asks that Facebook end its policy of exempting politicians from its hate speech guidelines and hire a C-suite executive.

"We've been down this road with Facebook so many times," said Jade Magnus Ogunnaiké, who is leading the campaign for the racial justice group Color of Change, noting that the boycott effort was a response to years of "fruitless" private meetings with Facebook staff as well as Zuckerberg. "At this point, we have reached an impasse."

Other brands joined after outreach from civil rights groups and their supporters, including Prince Harry and his wife Meghan, Duchess of Sussex, whose representatives contacted the head of the Anti-Defamation League recently to ask how they could help, said a spokesman for the organization.

The organizers of the boycott were also concerned about a post by President Trump, who appeared to endorse violence when he invoked a racially divisive phrase that dates to the civil rights era to describe the potential involvement of the U.S. military in the Minnesota protests. "When the looting starts, the shooting starts," he said on Twitter.

Facebook refused to take down the president's post, despite widespread protests by employees and outsiders, while Twitter slapped a warning label on it, noting that it violated the company's policies prohibiting incitement to violence. Snapchat stopped promoting the president's account.

Some smaller companies like Patreon that joined the boycott are an example of businesses that largely built on the ability of Facebook and others to help target specific groups of consumers.

As advertising migrated online over the past couple of decades from print and other media, advertisers lost control over the tone of the material alongside which their ads appeared. On social media, an ad could appear next to a racist post or one by a terrorist organization.

In 2017, Verizon, Walmart, Pepsi and other major brands suspended their ads on YouTube after reports that they had appeared alongside objectionable content promoting extremist or racist views. Last year, some advertisers boycotted YouTube after they saw their ads appear next to predatory and exploitative activity. As a result of the 2017 boycott, YouTube changed its policies and invested heavily in tools to give advertisers more control.

Katia Beauchamp, the co-founder and chief executive of the beauty box subscription company Birchbox, said the company, which is participating in the boycott, has committed to decreasing its ad spending with Facebook and Instagram for the rest of the year and is "aggressively" exploring other avenues for advertising. She called the decision a matter of "legacy."

"What we're most focused on is profiting from perpetuating prejudice, racism and hate," Beauchamp said. "We're not as focused on any reparations based on where our advertising shows up."

Facebook and other social media companies have extensive policies prohibiting hate speech, graphic violence and calls for violence, harassment and other ills, and have hired thousands of content moderators to enforce those policies. But the companies also give wide latitude to political expression across the board and have been reluctant to listen to organizer complaints. Objectionable content has spread as a result, causing flare-ups with advertisers.

Facebook has offered modest concessions to the boycott. At a town hall on June 26, Zuckerberg announced that the company would attach labels to some politicians' posts. In his most explicit terms to date, he said that it would take down posts by anyone who incited violence or suppressed voting rights and would label posts by politicians that break its other policies. The company has long had a policy that has allowed the spread of misinformation by politicians.

Facebook on Monday also agreed to an external audit of how it polices hate speech, a specific request by the boycott's organizers. Zuckerberg will meet with them next week, the Anti-Defamation League said. Other organizers include Color of Change, the NAACP and Common Sense.

In correspondence with advertisers and journalists, Facebook has cited a European Union report on hate speech that found that Facebook assessed more hate speech reports in 24 hours than Twitter or YouTube. Twitter spokesman Brian Poliakoff confirmed that it is also consulting with advertisers after Unilever said it would boycott all social media. "Over the past few years we've made significant investments to raise the bar on our responsibility and this continues to be our #1 priority," said YouTube spokesman Christopher Lawton.

Kevin Urrutia, co-founder of Voy Media, an ad agency specializing in Facebook ads, said most businesses are so reliant on Facebook that it's almost a nonissue: Less than 10 percent of his clients are participating in the boycott or are concerned about their relationships with the company. The other 90 percent hope it could result in cheaper ad purchases, he said.

"We have lots of clients that are pulling budget out this time of year," he said. "It could just be a matter of companies readjusting the budgets and using it as a way to get credibility with customers."

---- Index References ----

News Subject: (Business Management (1BU42); Minority & Ethnic Groups (1MI43); Race Relations (1RA49); Sales & Marketing (1MA51); Social Issues (1SO05))

Industry: (Advertising (1AD82); Advertising & Public Relations (1AD83); Advertising Expenditure (1AD68); Internet (1IN27); Internet Media (1IN67); Online Social Media (1ON38))

Region: (Americas (1AM92); Minnesota (1MI53); North America (1NO39); U.S. Midwest Region (1MI19); USA (1US73))

Language: EN

Word Count: 1900

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom

DEFENDANTS' EXHIBIT 151:

December 16, 2021

Feature

A Farewell to Dr. Francis Collins

Francis S. Collins, M.D., Ph.D., is stepping down as NIH director on December 19, 2021, after more than 12 years at the helm. A physician-geneticist, Dr. Collins took office as the 16th NIH director on August 17, 2009, after being appointed by President Barack Obama and confirmed by the U.S. Senate. In 2017, he was asked to continue in his role by President Donald Trump, and in 2021, by President Joe Biden. The longest serving presidentially appointed NIH Director, Dr. Collins' impact on biomedical research and the health of the nation is difficult to overstate. From launching the Brain Research Through Advancing Innovative Technologies (BRAIN) Initiative to spearheading NIH's response to the COVID-19 pandemic, Dr. Collins has steered the country's largest medical research agency with a calm hand, a scientific mind, and a deep commitment to the well-being of all Americans.

“Millions of people will never know Dr. Collins saved their lives. Countless researchers will aspire to follow in his footsteps. And I will miss the counsel, expertise, and good humor of a brilliant mind and dear friend.”

— President Joe Biden

[News Release: Collins to Step Down](#) | [NIH Record](#)



Francis S. Collins, M.D., Ph.D. *National Institutes of Health*

Video Tribute

More than 100 prominent figures from around the world created videos to pay tribute to Dr. Collins and wish him well as he transitions back to working in the lab at the National Human Genome Research Institute (NHGRI) and contemplates his next career steps. You also can watch individual videos using the Video Album directory.

A Virtual Farewell Tribute to NIH Director Dr. Francis ...



ACADEMIA, PUBLIC HEALTH, & SCIENTIFIC RESEARCH



THE ARTS



DIRECTORS OF NIH INSTITUTES & CENTERS



MEDIA



NIH STAFF — CURRENT



NIH STAFF — FORMER



NONPROFIT & ADVOCACY



PRIVATE-SECTOR



SPIRITUAL LEADERS



SPOUSE



U.S. GOVERNMENT OFFICIALS — CURRENT



U.S. GOVERNMENT OFFICIALS — FORMER



U.S. PRESIDENTS & VICE PRESIDENTS



This page last reviewed on December 6, 2022

NIH...Turning Discovery Into Health®

National Institutes of Health, 9000 Rockville Pike, Bethesda, Maryland 20892

U.S. Department of Health and Human Services

DEFENDANTS' EXHIBIT 152:

naturemedicine

[nature](#) > [nature medicine](#) > journal information

Journal Information

Nature Medicine is a monthly journal publishing original peer-reviewed research in all areas of medicine on the basis of its originality, timeliness, interdisciplinary interest and impact on improving human health. *Nature Medicine* also publishes commissioned content, including News, Reviews and Perspectives, aimed at contextualizing the latest advances in translational and clinical research to reach a wide audience of M.D. and Ph.D. readers. All editorial decisions are made by a team of full-time professional editors.

[Aims & Scope](#)

[Content Types](#)

[Clinical Research Guidelines](#)

[About the Editors](#)

[Contact](#)

Additional information

Journal abbreviation

The correct abbreviation for abstracting and indexing purposes is *Nat. Med.*


ISSN

Our international standard serial number (ISSN) is 1078-8956. Our electronic international standard serial number (EISSN) is 1546-170X.

Journal and article metrics

For a summary and description of the key journal and article metrics for Nature Medicine (including metrics on peer review turnaround times), visit our [Journal Metrics page](#).

Nature Medicine (*Nat Med*) | ISSN 1546-170X (online) | ISSN 1078-8956 (print)



DEFENDANTS' EXHIBIT 153:

NEWS AND EVENTS

Managing harmful vaccine content on YouTube

By The YouTube Team

Sep.29.2021



We're expanding our medical misinformation policies on YouTube with new guidelines on vaccines

Crafting policy around medical misinformation comes charged with inherent challenges and tradeoffs. Scientific understanding evolves as new research emerges, and firsthand, personal experience regularly plays a powerful role in online discourse. Vaccines in particular have been a source of fierce debate over the years, despite consistent guidance from health authorities about their effectiveness. Today, we're expanding our medical misinformation policies on YouTube with new [guidelines](#) on currently administered vaccines that are approved and confirmed to be safe and effective by local health authorities and the WHO.

Since last year we've

**SINCE LAST YEAR, WE'VE
removed over
130,000 videos for
violating our COVID-
19 vaccine policies.**

Our Community Guidelines already prohibit certain types of medical misinformation. We've long removed content that promotes harmful remedies, such as saying drinking turpentine can cure diseases. At the onset of COVID-19, we built on these policies when the pandemic hit, and worked with experts to develop 10 new policies around [COVID-19 and medical misinformation](#). Since last year, we've removed over 130,000 videos for violating our COVID-19 vaccine policies.

Throughout this work, we learned important lessons about how to design and enforce nuanced medical misinformation policies at scale. Working closely with health authorities, we looked to balance our commitment to an open platform with the need to remove egregious harmful content. We've steadily seen false claims about the coronavirus vaccines spill over into misinformation about vaccines in general, and we're now at a point where it's more important than ever to expand the work we started with COVID-19 to other vaccines.

Specifically, content that falsely alleges that approved vaccines are dangerous and cause chronic health effects, claims that vaccines do not reduce transmission or contraction of disease, or contains misinformation on the substances contained in vaccines will be removed. This would include content that falsely says that approved vaccines cause autism, cancer or infertility, or that substances in vaccines can track those who receive them. Our policies not only cover specific routine immunizations like

for measles or Hepatitis B, but also apply to general statements about vaccines.

As with our COVID guidelines, we consulted with local and international health organizations and experts in developing these policies. For example, our new guidance on vaccine side effects maps to public vaccine resources provided by health authorities and backed by medical consensus. These policy changes will go into effect today, and as with any significant update, it will take time for our systems to fully ramp up enforcement.

There are important exceptions to our new guidelines. Given the importance of public discussion and debate to the scientific process, we will continue to allow content about vaccine policies, new vaccine trials, and historical vaccine successes or failures on YouTube. Personal testimonials relating to vaccines will also be allowed, so long as the video doesn't violate other Community Guidelines, or the channel doesn't show a pattern of promoting vaccine hesitancy.

All of this complements our ongoing work to [raise up authoritative health information](#) on our platform and connect people with credible, quality health content and sources.

Today's policy update is an important step to address vaccine and health misinformation on our platform, and we'll continue to invest across the board in the policies and products that bring high quality information to our viewers and the entire YouTube community.

Related Topics

POLICY

YouTube Official Blog

Explore the latest company news, creator and artist profiles, culture and trends analyses, and behind-the-scenes insights on the YouTube Official Blog.

Our Channels



Twitter



Connect



About YouTube



YouTube Products



For Business



For Creators



Our Commitments




[Policy & Safety](#)

[Copyright](#)

[Brand Guidelines](#)

[Privacy](#)

[Terms](#)

 [Help](#)

[English](#)



DEFENDANTS' EXHIBIT 154:

DOJ 23-422 (D.O.J.), 2023 WL 2968014

Department of Justice (D.O.J.)

Federal Bureau of Investigation (FBI)

(NEWS RELEASE)

**40 OFFICERS OF CHINA'S NATIONAL POLICE CHARGED IN
TRANSNATIONAL REPRESSION SCHEMES TARGETING U.S. RESIDENTS**

April 17, 2023

**Defendants Accused of Creating Fake Social Media Accounts to Harass PRC Dissidents, and Working
with Employees of a U.S. Telecommunications Company to Remove Dissidents from Company's Platform**

Two criminal complaints filed by the U.S. Attorney's Office for the Eastern District of New York were unsealed today in federal court in Brooklyn charging 44 defendants with various crimes related to efforts by the national police of the People's Republic of China (PRC) - the Ministry of Public Security (MPS) - to harass Chinese nationals residing in the New York metropolitan area and elsewhere in the United States. The defendants, including 40 MPS officers and two officials in the Cyberspace Administration of China (CAC), allegedly perpetrated transnational repression schemes targeting U.S. residents whose political views and actions are disfavored by the PRC government, such as advocating for democracy in the PRC.

In the two schemes, the defendants created and used fake social media accounts to harass and intimidate PRC dissidents residing abroad and sought to suppress the dissidents' free speech on the platform of a U.S. telecommunications company (Company-1). The defendants charged in these schemes are believed to reside in the PRC or elsewhere in Asia and remain at large.

“These cases demonstrate the lengths the PRC government will go to silence and harass U.S. persons who exercise their fundamental rights to speak out against PRC oppression, including by unlawfully exploiting a U.S.-based technology company,” said Assistant Attorney General Matthew G. Olsen of the Justice Department's National Security Division. “These actions violate our laws and are an affront to our democratic values and basic human rights.”

“China's Ministry of Public Security used operatives to target people of Chinese descent who had the courage to speak out against the Chinese Communist Party - in one case by covertly spreading propaganda to undermine confidence in our democratic processes and, in another, by suppressing U.S. video conferencing users' free speech,” said Acting Assistant Director Kurt Ronnow of the FBI Counterintelligence Division. “We aren't going to tolerate CCP repression - its efforts to threaten, harass, and intimidate people - here in the United States. The FBI will continue to confront the Chinese government's efforts to violate our laws and repress the rights and freedoms of people in our country.”

Disclosure: U.S. Attorney Breon Peace for the Eastern District of New York is recused from and has not participated in the case captioned United States v. Julien Jin et al., 20-mj-1103.

United States v. Yunpeng Bai, et al.

The two-count complaint charges 34 MPS officers with conspiracy to transmit interstate threats and conspiracy to commit interstate harassment. All the defendants are believed to reside in the PRC, and they remain at large.

As alleged, the officers worked with Beijing's MPS bureau and are or were assigned to an elite task force called the "912 Special Project Working Group" (the Group). The purpose of the Group is to target Chinese dissidents located throughout the world, including in the United States.

"As alleged, the PRC government deploys its national police and the 912 Special Project Working Group not as an instrument to uphold the law and protect public safety, but rather as a troll farm that attacks persons in our country for exercising free speech in a manner that the PRC government finds disagreeable, and also spreads propaganda whose sole purpose is to sow divisions within the United States," said U.S. Attorney Breon Peace for the Eastern District of New York. "I commend the investigative team for comprehensively revealing the insidiousness of a state-directed criminal scheme directed at residents of the United States."

The complaint alleges how members of the Group created thousands of fake online personas on social media sites, including Twitter, to target Chinese dissidents through online harassment and threats. These online personas also disseminated official PRC government propaganda and narratives to counter the pro-democracy speech of the Chinese dissidents. As alleged, for example, Group members created and maintained the fake social media accounts through temporary email addresses, posted official PRC government content, and interacted with other online users to avoid the appearance that the Group accounts were "flooding" a given social media platform. The Group tracks the performances of members in fulfilling their online responsibilities and rewards Group members who successfully operate multiple online personas without detection by the social media companies who host the platforms or by other users of the platforms.

The investigation also uncovered official MPS taskings to Group members to compose articles and videos based on certain themes targeting, for example, the activities of Chinese dissidents located abroad or the policies of the U.S. government.

As alleged, the defendants also attempted to recruit U.S. persons to act as unwitting agents of the PRC government by disseminating propaganda or narratives of the PRC government. On several occasions, the defendants used online personas to contact individuals assessed to be sympathetic and supportive of the PRC government's narratives and asked these individuals to disseminate Group content.

In addition, Group members took repeated affirmative actions to have Chinese dissidents and their meetings removed from the platform of Company-1. For example, Group members disrupted a dissident's efforts to commemorate the Tiananmen Square Massacre through a videoconference by posting threats against the participants through the platform's chat function. In another Company-1 videoconference on the topic of countering communism organized by a PRC dissident, Group members flooded the videoconference and drowned out the meeting with loud music and vulgar screams and threats directed at the pro-democracy participants.

United States v. Julien Jin, et al.

This amended complaint charges 10 individuals, including a former PRC-based Company-1 employee, six MPS officers, and two officials with the CAC, with conspiracy to commit interstate harassment and unlawful conspiracy to transfer means of identification. Nine of the defendants are believed to reside in the PRC and remain at large. The tenth defendant is believed to reside in Indonesia or the PRC and also remains at large.

"The amended complaint charging a former PRC-based employee of a U.S. telecommunications company illustrates the insider threat faced by U.S. companies operating in the PRC," said First Assistant U.S. Attorney Pokorny for the Eastern District of New York, who thanked Company-1 for its cooperation in the government's investigation. "As alleged, Julien Jin and his co-conspirators in the Ministry of Public Security and Cyberspace Administration of China weaponized the U.S. telecommunications company he worked for to intimidate and silence dissenters and enforce PRC law to the detriment of Chinese activists in New York, among other places, who had sought refuge in this country to peacefully express their pro-democracy views."

“These cases demonstrate that the Chinese Communist Party, once again, attempted to intimidate, harass, and suppress Chinese dissidents in the United States,” said Assistant Director in Charge David Sundberg of the FBI Washington Field Office. “In the United States, the freedom of speech is a cornerstone of our democracy, and the FBI will work tirelessly to defend everyone's right to speak freely without fear of retribution from the CCP. These complex investigations revealed an MPS-wide effort to repress individuals by using the U.S. communications platform and fake social media accounts to censor political and religious speech.”

In December 2020, the Department first announced charges against Julien Jin in connection with his efforts to disrupt a series of meetings on the Company-1 platform held in May and June 2020 commemorating the 1989 Tiananmen Square Massacre. Jin served as Company-1's primary liaison with PRC government law enforcement and intelligence services. In that capacity, he regularly responded to requests from the PRC government to terminate meetings and block users on Company-1's video communications platform.

As detailed in the original complaint, Jin and others conspired to use Company-1's U.S. systems to censor the political and religious speech of individuals located in the United States and elsewhere at the direction of the PRC government. For example, Jin and others disrupted meetings held on the Company-1 platform to discuss politically sensitive topics unacceptable to the PRC government - including the Tiananmen Square Massacre. Jin and his co-conspirators fabricated evidence of purported misconduct to cause U.S.-based employees of Company-1 to terminate the meetings.

The allegations in the amended complaint reveal that Jin worked directly with and took orders from defendants at the MPS and the CAC to disrupt meetings on the Company-1 platform and that the co-defendants had targeted U.S.-based dissidents' speech on Company-1's platform since 2018.

Starting in 2018, Jin and his co-defendants repeatedly sought to terminate video chat meetings organized by a Chinese dissident residing in New York City who has been a vocal critic of the PRC government and the Chinese Communist Party. After the CAC requested that Company-1 terminate the dissident's meetings on the Company-1 platform, Jin worked to identify all accounts associated with the dissident, caused meetings related to the dissident to be hosted in a “quarantine zone” - that is, on a server with known lags in response time - and later worked to block all accounts associated with the dissident. Similarly, in 2019, Jin collaborated with the MPS and CAC to block accounts seeking to commemorate the Tiananmen Square Massacre.

The FBI Washington Field Office investigated the cases.

Assistant U.S. Attorneys Alexander A. Solomon, Antoinette N. Rangel, Ian C. Richardson, Nicholas J. Moscow and Jessica K. Weigel of the Eastern District of New York, and Trial Attorney Scott A. Claffee of the National Security Division's Counterintelligence and Export Control Section are prosecuting the cases.

The FBI has created a website for victims to report efforts by foreign governments to stalk, intimidate, or assault people in the United States. Please visit: www.fbi.gov/investigate/counterintelligence/transnational-repression.

DOJ 23-422 (D.O.J.), 2023 WL 2968014

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 155:

NewsRoom

3/30/23 WashingtonPost.com (Pg. Unavail. Online)
2023 WLNR 11432730

WashingtonPost.com
Copyright (c) 2023 The Washington Post

March 30, 2023

Section: /national-security

Secret trove offers rare look into Russian cyberwar ambitions

Craig Timberg; Ellen Nakashima; Hannes Munzinger; Hakan Tanriverdi

Russian intelligence agencies worked with a Moscow-based defense contractor to strengthen their ability to launch cyberattacks, sow disinformation and surveil sections of the internet, according to thousands of pages of confidential corporate documents.

The documents detail a suite of computer programs and databases that would allow Russia's intelligence agencies and hacking groups to better find vulnerabilities, coordinate attacks and control online activity. The documents suggest the firm was supporting operations including both social media disinformation and training to remotely disrupt real-world targets, such as sea, air and rail control systems.

An anonymous person provided the documents from the contractor, NTC Vulkan, to a German reporter after expressing outrage about Russia's attack on Ukraine. The leak, an unusual occurrence for Russia's secretive military industrial complex, demonstrates another unintended consequence of President Vladimir Putin's decision to take his country to war.

Officials from five Western intelligence agencies and several independent cybersecurity companies said they believe the documents are authentic, after reviewing excerpts at the request of The Washington Post and several partner news organizations.

These officials and experts could not find definitive evidence that the systems have been deployed by Russia or been used in specific cyberattacks, but the documents describe testing and payments for work done by Vulkan for the Russian security services and several associated research institutes. The company has both government and civilian clients.

The trove offers a rare window into the secret corporate dealings of Russia's military and spy agencies, including work for the notorious government hacking group Sandworm. U.S. officials have accused Sandworm of twice causing power blackouts in Ukraine, disrupting the Opening Ceremonies of the 2018 Winter Olympics and launching NotPetya, the most economically destructive malware in history.

One of the leaked documents mentions the numerical designation for Sandworm's military intelligence unit, 74455, suggesting that Vulkan was preparing software for use by the elite hacking squad. The unsigned, 11-page document, dated 2019, showed a Sandworm official approving the data transfer protocol for one of the platforms.

"The company is doing bad things, and the Russian government is cowardly and wrong," said the person who provided the documents to the German reporter, shortly after the invasion of Ukraine. The reporter then shared them with a consortium

of news organizations, which includes The Washington Post and is led by Paper Trail Media and Der Spiegel, both based in Germany.

The anonymous person, who spoke to the reporter through an encrypted chat app, declined to identify themselves before ending contact, declaring the need to vanish "like a ghost" for security reasons.

"I am angry about the invasion of Ukraine and the terrible things that are happening there," the person said. "I hope you can use this information to show what is happening behind closed doors."

Vulkan did not respond to requests for comment. An employee of the company who answered the phone at its head office confirmed that an email with queries had been received and said it would be answered by company officials, "if it is of interest to them."

No responses came. Kremlin officials also did not reply to requests for comment.

The cache of more than 5,000 pages of documents, dated between 2016 and 2021, includes manuals, technical specification sheets and other details for software that Vulkan designed for the Russian military and intelligence establishment. It also includes internal company emails, financial records and contracts that show both the ambition of Russia's cyber operations and the breadth of the work Moscow has been outsourcing.

This includes programs to create fake social media pages and software that can identify and stockpile lists of vulnerabilities in computer systems across the globe for possible future targeting.

Several mock-ups of a user interface for a project known as Amezit appear to depict examples of possible hacking targets, including the Foreign Ministry in Switzerland and a nuclear power plant in that nation. Another document shows a map of the United States with circles that appear to represent clusters of internet servers.

One illustration for a Vulkan platform called Skan makes reference to a U.S. location, labeled "Fairfield," as a place to find network vulnerabilities for use in an attack. Another document describes a "user scenario" in which hacking teams would identify insecure routers in North Korea, presumably for potential use in a cyberattack.

The documents do not, however, include verified target lists, malicious software code or evidence linking the projects to known cyberattacks. Still, they offer insights into the aims of a Russian state that — like other major powers, including the United States — is eager to grow and systematize its ability to conduct cyberattacks with greater speed, scale and efficiency.

"These documents suggest that Russia sees attacks on civilian critical infrastructure and social media manipulation as one and the same mission, which is essentially an attack on the enemy's will to fight," said John Hultquist, the vice president for intelligence analysis at the cybersecurity firm Mandiant, which reviewed selections of the document at the request of The Post and its partners.

'A critical pillar'

The role of contractors in Russian cyberwarfare is "very significant," especially for the Russian military intelligence agency commonly called the GRU, said a Western intelligence analyst, speaking on the condition of anonymity to share sensitive findings. "They are a critical pillar of GRU offensive cyber research and development. They provide expertise that the GRU may lack on a given issue. The spy services can do cyber operations without them, but likely not as well."

Three former Vulkan employees, who spoke on the condition of anonymity out of fear of retribution, confirmed some details about the company. Financial records for Vulkan, which were separately obtained by the news organizations, match references

in the documents in several instances, detailing millions of dollars worth of transactions between known Russian military or intelligence entities and the company.

The intelligence and cybersecurity experts said details in the documents also match information collected about Russia's hacking programs — including in a smaller previous leak — and appear to describe new tools for enabling offensive cyber operations. Vulkan, they said, is one of dozens of private firms known to provide tailored cyber capabilities to the Russian security services.

The experts cautioned that it was not clear which of the programs had been completed and deployed, as opposed to being merely developed and ordered up by the Russian military, including by units linked to the GRU. The documents do, however, refer to state-mandated testing, changes desired by the clients and finished projects, strongly suggesting that at least trial versions of some of the programs were activated.

"You don't find network diagrams and design documents like this very often. It really is very intricate stuff. This wasn't meant to be ever seen publicly," said one of the Western intelligence officials, speaking on the condition of anonymity to share candid assessments of sensitive findings. "But it makes sense to pay attention. Because you better understand what the GRU is trying to do."

The Threat Analysis Group at Google, the tech company's premier cyberthreat hunter, found evidence in 2012 that Vulkan was being used by the SVR, Russia's foreign intelligence service. The researchers observed a suspicious test phishing email being sent from a Gmail account to a Vulkan email account that had been set up by the same person, evidently a company employee.

"[T]he use of test messages is common practice to test phishing emails prior to their use," Google said in a statement. After that test email, the Google analysts saw the same Gmail address being used to send malware known to be employed by SVR against other targets.

That was "not the smartest move" on the Vulkan employee's part, said one Google analyst, speaking on the condition of anonymity to describe sensitive findings. "It was definitely a slip-up."

References to the company also can be found in VirusTotal, a Google-owned service with a database of malicious software that is a resource for security researchers.

A file labeled "Secret Party NTC Vulkan" is a holiday invitation disguised in a piece of malware that normally takes control of a user's computer. The invitation — apparently harmless — automatically downloads an illustration of a large bear alongside a champagne bottle and two glasses.

The image is labeled "APT Magma Bear," a reference to Western cybersecurity officials' labeling of Russian hacking groups with ursine code names. APT refers to "Advanced Persistent Threat," a cybersecurity term for the most serious hacking groups, which are typically run by nation states such as Russia.

The invitation reads "APT Magma Bear wishing you and your family a wonderful holiday season and a healthy and peaceful New Year!" as Soviet military music plays in the background.

Ties to Western corporations

Vulkan was founded in 2010 and has about 135 employees, according to Russian business information websites. The company website says its main headquarters is in northeast Moscow.

A promotional video on the company website portrays Vulkan as a scrappy tech start-up that "solves corporate problems" and has a "comfortable work environment." It ends by declaring that Vulkan's goal is to "make the world a better place."

The promotional video does not mention military or intelligence contracting work.

"The work was fun. We used the latest technologies," said one former employee in an interview, speaking on the condition of anonymity for fear of retribution. "The people were really clever. And the money was good."

Some former Vulkan employees later worked for major Western companies, including Amazon and Siemens. Both companies issued statements that did not dispute that former Vulkan employees worked for them, but they said that internal corporate controls protected against unauthorized access to sensitive data.

The documents also show that Vulkan intended to use an array of U.S. hardware in setting up systems for Russian security services. The design documents repeatedly refer to American products, including Intel processors and Cisco routers, that should be used to configure the "hardware-software" systems for Russian military and intelligence units.

There are other connections to U.S. companies. Some of those companies, including IBM, Boeing and Dell at one time worked with Vulkan, according to its website, which describes commercial software development work with no obvious ties to intelligence and hacking operations. Representatives of IBM, Boeing and Dell did not dispute that those entities previously worked with Vulkan but said they do not now have any business relationships with the company.

Automated disinformation

The trove of documents initially was shared with a reporter for the German newspaper Süddeutsche Zeitung. The consortium examining the documents has 11 members — including The Post, the Guardian, Le Monde, Der Spiegel, iStories, Paper Trail Media and Süddeutsche Zeitung — from eight countries.

Among the thousands of pages of leaked Vulkan documents are projects designed to automate and enable operations across Russian hacking units.

Amezit, for example, details tactics for automating the creation of massive numbers of fake social media accounts for disinformation campaigns. One document in the leaked cache describes how to use banks of mobile phone SIM cards to defeat verification checks for new accounts on Facebook, Twitter and other social networks.

Reporters for Le Monde, Der Spiegel and Paper Trail Media, working from Twitter accounts listed in the documents, found evidence that these tools probably had been used for numerous disinformation campaigns in several countries.

One effort included tweets in 2016 — when Russian disinformation operatives were working to boost Republican presidential candidate Donald Trump and undermine Democrat Hillary Clinton — linking to a website claiming that Clinton had made "a desperate attempt" to "regain her lead" by seeking foreign support in Italy.

The reporters also found evidence of the software being used to create fake social media accounts, inside and outside of Russia, to push narratives in line with official state propaganda, including denials that Russian attacks in Syria killed civilians.

Amezit has other features designed to allow Russian officials to monitor, filter and surveil sections of the internet in regions they control, the documents show. They suggest that the program contains tools that shape what internet users would see on social media.

The project is repeatedly described in the documents as a complex of systems for "information restriction of the local area" and the creation of an "autonomous segment of the data transmission network."

A 2017 draft manual for one of the Amezit systems offers instructions on the "preparation, placement and promotion of special materials" — most likely propaganda distributed using fake social media accounts, telephone calls, emails and text messages.

Mapping critical infrastructure

One of the mock-ups in a 2016 design document allows a user to hover a cursor over an object on a map and display IP addresses, domain names and operating systems as well as other information about "physical objects."

One such physical object — highlighted in fluorescent green — is the Ministry of Foreign Affairs in Bern, Switzerland, which shows a hypothetical email address and the "attack goal" to "obtain root user privileges." The other object highlighted on the map is the Muhleberg Nuclear Power Plant, west of Bern. It stopped producing power in 2019.

Dmitri Alperovitch, who co-founded the cyberthreat intelligence firm CrowdStrike, said that the documents indicate that Amezit is intended to enable discovery and mapping of critical facilities such as railways and power plants, but only when the attacker has physical access to a facility.

"With physical access, you can plug this tool into a network and it will map out vulnerable machines," said Alperovitch, now the chairman of Silverado Policy Accelerator, a think tank in Washington.

Emails suggest that the Amezit systems were at least tested by Russian intelligence agencies by 2020. A company email dated May 16, 2019, describes feedback from the customer and desires for changes in the program. A spreadsheet marks which parts of the project have been finished.

A document in the trove also suggests that Vulkan was contracted in 2018 to create a training program called Crystal-2 to provide simultaneous operation by up to 30 trainees. The document mentions testing "the Amezit system to disable [incapacitate] control systems for rail, air and sea transport" but does not make clear whether the training program conceived in the documents went forward.

Trainees also would be "testing methods for obtaining unauthorized access to local computer and technological networks of infrastructure and facilities to support life in population centers and industrial areas," potentially using capabilities the document ascribes to Amezit.

Later in the document, the text reads: "The level of secrecy of processed and stored information in the product is 'Top Secret.'"

Repository of vulnerabilities

Skan, the other main project described in the documents, allowed Russia's attackers continuously to analyze the internet for vulnerable systems and compile them in a database for possible future attacks.

Joe Slowik, the threat intelligence manager at the cybersecurity company Huntress, said Skan probably was designed to work in tandem with other software.

"This is the background system that would allow for it all — organizing and potentially tasking and targeting of capabilities in a way that can be centrally managed," he said.

Slowik said Sandworm, the Russian military hacking group blamed for numerous disruptive attacks, was likely to want to keep a large repository of vulnerabilities. A document from 2019 says Skan could be used to display "a list of all possible attack scenarios" and highlight all the nodes on the network that could be involved in the attacks.

The system also appears to enable coordination among Russian hacking units, allowing "the ability to exchange data between prospective geographically dispersed special units," according to the leaked documents.

"Skan reminds me of old military movies where people stand around ... and place their artillery and troops on the map," says Gabby Roncone, another cybersecurity expert at Mandiant. "And then they want to understand where the enemy tanks are and where they need to strike first to break through the enemy lines."

There is evidence that at least some part of Skan was delivered to the Russian military.

In an email dated May 27, 2020, Vulkan developer Oleg Nikitin described collecting a list of employees "to visit the territory of our functional user" to install and configure equipment for the Skan project, and upgrade and configure software and demonstrate functionality. The functional user is described as "Khimki," a reference to the Moscow suburb where Sandworm is based.

"The territory is closed, the regime is strict," Nikitin wrote, using Russian terms for a protected, secret government facility.

Nikitin did not reply to a request for comment.

Maria Christoph from Paper Trail Media contributed to this report.

Craig Timberg is The Post's senior editor for collaborative investigations and a former technology reporter. Ellen Nakashima is a Post national security reporter who has written about cybersecurity and intelligence issues. Hannes Munzinger and Hakan Tanriverdi are senior investigative reporters for Paper Trail Media, based in Munich. Munzinger received the document trove and had initial conversations with the source while working for his previous employer, Süddeutsche Zeitung.

---- Index References ----

Company: DER SPIEGEL GmbH & Co. KG; INTERNATIONAL BUSINESS MACHINES CORPORATION; AMAZON.COM, INC.; Ministry of Foreign Affairs

News Subject: (Cybercrime & Viruses (1CY34); Emerging Market Countries (1EM65))

Industry: (Aerospace & Defense (1AE96); Defense (1DE43); Defense Intelligence (1DE90); Electronic & Information Warfare (1EL90); Internet (1IN27); Internet Security (1IN07); Security (1SE29); Security Agencies (1SE35); Security Software (1SE53))

Region: (Asia (1AS61); CIS Countries (1CI64); Central Europe (1CE50); Eastern Europe (1EA48); Europe (1EU83); Eurozone Countries (1EU86); Germany (1GE16); Russia (1RU33); Switzerland (1SW77); Ukraine (1UK09); Western Europe (1WE41))

Language: EN

Other Indexing: (Cisco; Dell; NTC Vulkan; Paper Trail Media; Foreign Ministry; Threat Analysis Group; Silverado Policy Accelerator; Der Spiegel; IBM; Amazon; Ministry of Foreign Affairs)

Word Count: 2822

End of Document

© 2023 Thomson Reuters. No claim to original U.S. Government Works.

NewsRoom

DEFENDANTS' EXHIBIT 156:

DECEMBER 21, 2021

Remarks by President Biden on the Fight Against COVID-19

State Dining Room

2:42 P.M. EST

THE PRESIDENT: Good afternoon. I promised when I got elected that I'd always give it to you straight from the shoulder — the good, the bad, the truth.

So, as we head into Christmas weekend, I want to answer your questions about the rising number of COVID cases — COVID-19 cases.

And I want to start by acknowledging how tired, worried, and frustrated I know you are. I know how you're feeling.

For many of you, this will be the first or even the second Christmas where you look — across the table will be an empty kitchen chair there.

Tens of millions have gotten sick, and we've all experienced an upheaval in our lives.

But while COVID has been a tough adversary, we've shown that we're tougher — tougher because we have the power of science and vaccines that prevent illness and save lives, and tougher because of our resolve.

So, that — let me answer some questions that lay out the steps the Vice President and I are taking to prepare for the rising number of cases experts tell us we could expect in the weeks ahead.

First, how concerned should you be about Omicron, which is now the dominant variant in this country and it happened so quickly?

The answer is straightforward: If you are not fully vaccinated, you have good reason to be concerned. You're at a high risk of getting sick. And if you get sick, you're likely to spread it to

others, including friends and family. And the unvaccinated have a significantly higher risk of ending up in a hospital or even dying.

Almost everyone who has died from COVID-19 in the past many months has been unvaccinated. Unvaccinated.

But if you're among the majority of Americans who are fully vaccinated, and especially if you've gotten the booster shot — that third shot — you're much — you have much, much less reason to worry. You have a high degree of protection against severe illness.

And because Omicron spreads so easily, we'll see some fully vaccinated people get COVID, potentially in large numbers. There will be positive cases in every office, even here in the White House, among the unv- — among the vaccinated — among the vaccinated — from Omicron.

But these cases are highly unlikely to lead to serious illness.

Vaccinated people who get COVID may get ill, but they're protected from severe illness and death. That's why you should still remain vigilant.

According to our doctors, even if you're fully vaccinated, you should wear a mask when indoors in public settings.

Wearing a mask provides extra protection for you and those around you. And I know some Americans are wondering if you can safely celebrate the holidays with your family and friends.

The answer is yes, you can, if you and those you celebrate with are vaccinated, particularly if you've gotten your booster shot.

If you are vaccinated and follow the precautions that we all know well, you should feel comfortable celebrating Christmas and the holidays as you planned it.

You know, you've done the right thing. You could enjoy the holiday season.

And thanks to the progress on vaccinations this fall, we've gone from nearly 90 million adults in July who had not even started their vaccination process to fewer than 40 million today. Still too many, but down from 90 to 40.

All these people who have not been vaccinated, you have an obligation to yourselves, to your family, and, quite frankly — I know I'll get criticized for this — to your country.

Get vaccinated now. It's free. It's convenient. I promise you, it saves lives. And I, honest to God, believe it's your patriotic duty.

Another question folks are asking is: What can you do to make yourself and your family feel safer and be safer? The answer is simple: Get your booster shot. Wear a mask.

Our doctors have made it clear: Booster shots provide the strongest of protections. Unfortunately, we still have tens of millions of people who are eligible for the booster shot who have not yet gotten it. They've gotten the first two shots, but they've not gotten the booster.

Folks, the booster shots are free and widely available. Over 60 million Americans, including 62 percent of eligible seniors, our most vulnerable group, have gotten their booster shots.

I got my booster shot as soon as they were available. And just the other day, former President Trump announced he had gotten his booster shot. It may be one of the few things he and I agree on.

People with booster shots are highly protected. Join them. Join us. It's been six months or more since my second shot. If it's been six months or more for your second shot — when I got my booster — you can get yours today if you've been six months or more since your second shot.

Another question that folks are asking is: Are we going back to March 2020 — not this last March 2021, but March 2020 — when the pandemic first hit? That's what I keep getting asked.

The answer is absolutely no. No.

Here are three big differences between then and now: One — number one — the first one — more than 200 million Americans have been fully vaccinated. In March of 2020, no one was fully vaccinated. What that means is, today, as cases — a case of COVID-19 for a fully vaccinated and boosted person will most likely mean no symptoms or mild ones similar to the common respiratory viruses.

Over 200 million Americans should have the peace of mind that they did not have in March of 2020: They're protected from hospitalization, and they're protected from death.

Second point: We're prepared today for what's coming. In March of 2020, we were not ready. Today, we've spocktiled [sic] enough — we've stockpiled enough gowns, masks, and ventilators to deal with the surge of hospitalizations among the unvaccinated.

Today, we're ready.

And as I'll explain in a few minutes, we're going to be reinforcing our hospitals, helping them.

Number three, we know a lot more today than we did back in March of 2020. For example, last year, we thought the only way to keep your children safe was to close your — close our schools.

Today, we know more and we have more resources to keep those schools open. We can — you can get 5- to 11-year-olds vaccinated — a tool we didn't have until last month.

Today, we don't have to shut down schools because of a case of COVID-19. Now, if a student tests positive, other students can take the test and stay in the classroom if they're not infected rather than closing the whole school or having to quarantine.

We can keep our K-through-12 schools open, and that's exactly what we should be doing.

So, folks, let me summarize: We should all be concerned about Omicron but not panicked. If you're fully vaccinated, and especially if you got your booster shot, you are highly protected. And if you're unvaccinated, you're at higher risk of getting severely ill from COVID-19, getting hospitalized, and even dying.

So, the best thing to do is get fully vaccinated and get your booster shot.

And, no, this is not March of 2020. Two hundred million people are fully vaccinated. We're prepared. We know more. We just have to stay focused. So that's where we stand.

Now, let me tell you about the additional steps I'm ordering today to take on what is coming. I know you've heard a lot of this in the news already this morning.

Three weeks ago, I laid out a COVID-19 Action Plan for this winter that prepared us for this moment. Today, we're making the plan even stronger.

First, we're setting up our vaccination and booster efforts — we're stepping it up significantly. In the past two weeks, we've seen the highest vaccination rates since last spring. And we aren't as vaccinated, as a country, as we should be, though. That's why we have added 10,000 new vaccination sites on top of the 80,000 sites that are already we had — we already had in place, and even more will open in January.

I know there are some parts of this country where people are very eager to get their booster, where it's harder to get an appointment. Excuse me. (Coughs.)

So starting this week, I'll be deploying hundreds more vaccinators and more sites to help get the booster shots in people's arms.

I've ordered FEMA — the Federal Emergency Management Agency -- to stand up new pop-up vaccination clinics all across the country where you can get that booster shot.

We've opened — (coughs) — excuse me — we've opened FEMA vaccination sites in Washington State and New Mexico recently as cases have increased. And today, I'm directing FEMA to stand up new sites in areas where there is high demand.

These steps are going to help us add more — more and more booster appointments in over — just over the next few weeks.

I also want to say a word to parents: If your children are not vaccinated, please get them vaccinated. If you're a parent -- understandably — who waited to see how the first shots went with other kids before getting your own kid vaccinated, you can stop waiting. Six million children in our country ages 5 to 11 are vaccinated. Get your children protected today — now.

And for those parents out there who have a child that's too young to be vaccinated — that is under the age of five — I know this can still be a scary time. But one thing — one thing you can and must do while we await vaccines for children under five: Get yourself fully vaccinated and boosted, as well as those around you — your children, your caregivers, your siblings.

It's critical to mask up in public indoor places.

We know that our youngest children have only rarely been impacted by serious COVID cases — COVID-19 cases, but they can be further protected if they're surrounded by vaccinated people.

And again, to folks who are not vaccinated: You may think you're putting only yourself at risk, but it's your choice. Your choice is not just a choice about you; it affects other people. You're putting other people at risk — your loved ones, your friends, neighbors, strangers you run into. And your choice can be the difference between life or death.

The longer the virus is around, the more likely variants form that may be deadlier than the ones that have come before.

Let me say again and again and again and again: Please get vaccinated. It's the only responsible thing to do. And those who are not vaccinated are causing hospitals to overrun — become overrun again.

I just spoke to the governor of New York. Every COVID-19 hospital [hospitalization] means someone with a heart attack, cancer, or other serious illness may not get that bed and that lifesaving care they need in the hospital.

Look, let me give it to you straight again: Omicron is serious, potentially deadly business for unvaccinated people.

Let me be clear: Thanks to the prior administration and our scientific community, America is one of the first countries to get the vaccine. And thanks to my administration and the hard work of Americans, we led a rollout that made America among the world leaders in getting shots in arms.

But uptake slowed this summer as vaccine resistance among some hardened. Look, the unvaccinated are responsible

for their own choices. But those choices have been fueled by dangerous misinformation on cable TV and social media.

You know, these companies and personalities are making money by peddling lies and allowing misinformation that can kill their own customers and their own supporters.

It's wrong, it's immoral, and I call on the purveyors of these lies and misinformation to stop it. Stop it now.

One of the other things that we know that has to be done is more testing. Because Omicron spreads easily, especially among the unvaccinated, it's critically important that we know who's infected. That means we need more testing.

And on that score, we are ~~now~~ [not] where we should be.

Yes, we have over 20,000 free testing sites. Yes, we've used the Defense Production Act and spent \$3 billion to greatly expand the number of at-home tests available for purchase online and at your local pharmacy. And, yes, we've made sure insurance covers the PCR tests you get in a hospital or at your doctor's office.

But, starting next month, private insurance will all cover — also cover at-home testing so you can order a test online and get reimbursed. We're providing access to free at-home tests for those who may have insurance as well — may not have insurance, I should say, as well.

But it's not enough. We have to do more. We have to do better, and we will.

Starting this week, the federal government will set up emergency testing sites in areas that need additional testing capacity. Before Christmas, the first several of these federal testing sites will be up and running in New York City with many more to come.

This free testing is going to help reduce the waiting lines — the time you have to stand there and — and sometimes it's an hour or more.

We're going to continue to add federal testing sites where needed so that if you want an immediate test, there will be a place where you can go get it.

We also need to do better with at-home testing. So, I'm announcing today: The federal government will purchase one half billion — that's not million; billion with a "B" — additional at-home rapid tests, with deliveries starting in January.

We'll be getting these tests to Americans for free. And we'll have websites where you can get them delivered to your home.

We have arranged for it to be easier for you to find a free COVID testing site near you on Google. Just enter "COVID test near me" in the Google search bar and you can find a number of different locations nearby where you can get tested.

And we're going to continue to use the Defense Production Act as we did earlier this month to make sure we're producing as many tests and as quickly as possible.

The bottom line is it's a lot better than it was, but we're taking even more steps to make it easier to get tested and get tested for free.

Next, we are preparing hospitals for what's coming. Those 40 [million] unvaccinated adults have a good chance of getting COVID-19, and some of you will get very sick. That will mean hospitals are going to get extremely stressed — extremely stressed again, both in terms of equipment as well as personnel to care for those who get sick.

That's why my administration has stockpiled and pre-positioned millions of gowns, gloves, masks, and ventilators. We used to call it PPP [PPE]. We're ready to send them immediately to any state that needs more.

In addition, I have directed the Pentagon to mobilize an additional 1,000 troops to be deployed to help staff local hospitals and expand capacity. That's 1,000 military doctors, nurses, and medics. We've already started moving — military — excuse me, medical teams. They've already landed in Wisconsin and Indiana this week.

And this is on top of 300 federal medical — medical personnel that are now on the ground, having deployed since we learned about Omicron.

Look, while we know staffing is the biggest need for our hospitals, some may need more beds as well. We're prepared. I've directed FEMA to activate the National Response Center and begin deploying teams now to provide additional hospital beds. We'll begin to construct emergency capacity near hospitals, in parking garages, and nearby buildings to be ready if needed.

And the federal [sic] — the federal government is paying for all of this — period — all of it.

Further, FEMA will deploy hundreds of ambulances and EMS crews so that if one hospital fills up, we can transport patients to beds elsewhere.

This week, we will send dozens of ambulances to New York and Maine, because of the — because the COVID is spreading very rapidly, to help transport patients.

Our doctors, nurses, hospital staffs have gone above and beyond during this pandemic. The strain and stress is real. I really mean it. It's real. And we'll have their backs though. We have to let them know we have their backs.

Finally, we're making sure that COVID-19 no longer closes businesses or schools. Last week, the federal court reinstated my administration's vaccination-or-test — the vaccination-or-test rule for businesses with more than 100 employees.

The rule requires employers with 100 or more employees

to protect their workers who are on site and indoors with a requirement that they be vaccinated or tested each week or go home.

These rules are going to keep workers safe. And keep workers safe will help keep businesses open. If people are vaccinated or tested, they are much less likely to get sick and less likely to spread it to others. Customers are more likely to come in and shop because they know it's a safe environment.

I know vaccination requirements are unpopular for many. They're not even popular for those who are anxious to get them.

But my administration has put them in place not to control your life, but to save your life and the lives of others. Over 400,000 Americans died from COVID this calendar year — and almost

all were unvaccinated, almost all were preventable.

The rule is legal and effective, and it's going to save thousands of American lives.

We must also keep our K-12 schools open. Look, the science is clear and overwhelming. We know how to keep our kids safe from COVID-19 in school. K-through-12 schools should be open. And that safety is increased if schools require all adults who work in the schools to get vaccinated and take the safety measures that CDC has recommended, including masking.

I got Congress to pass billions of dollars in school improvements, ventilation, and social distancing. Schools should be safer than ever from COVID-19.

And just Friday, the CDC issued test-to-stay guidelines, so schools can stay open and kids can stay in class even if a classmate tests positive.

COVID-19 is scary. But the science is clear: Children are as safe as — are — as safe in school as they are anyplace, assuming the appropriate precautions have been taken, and they've already been funded.

Let me close with this: I know you're tired — I really mean this — and I know you're frustrated. We all want this to be over. But we're still in it, and this is a critical moment. But we also have more tools than we've ever had before.

We're ready. We'll get through this.

As we head into the holidays, I want us to all keep the faith.

I want to sincerely thank you for your perseverance, your courage, your countless acts of kindness, love, and sacrifice during these last two years.

Throughout our history, we've been tested as a people and as a nation. Through war and turmoil, we had to ask whether we'd be safe, whether we'd be okay, whether we'd be — get back to who we are.

We've always endured because we remember there is no challenge too big for America — I mean this from the bottom of my heart — no challenge.

We've come through better and stronger because we stay together as the United States of America.

That's what we have to keep doing today. We can do this together, I guarantee you.

May God bless you all, and may God protect our troops. And happy holidays. God love you all. Thank you.

Q Mr. President, on testing, sir, you said, “We have to do better.” But public health officials have been saying, for months, you need to surge rapid test for just this moment.

Is it a failure that you don’t have an adequate amount of tests for everyone to be able to get one if they need one right now?

THE PRESIDENT: No, it’s not, because COVID is spreading so rapidly, if you notice. It just — just happened almost overnight, just in the last month. And —

Q What’s your message —

THE PRESIDENT: I’m going to answer his question.

Q Mr. Pres- —

THE PRESIDENT: And so, no, it’s not a failure, but the alarm bell went off. I don’t think anybody anticipated that this was going to be as rapidly spreading as it did.

And so, the question is: We had a lot of people who have access to a test, who could order them, could — could have their insurance pay for them, et cetera.

But it all started — all of a sudden, it was like everybody rushed to the counter. There was a big, big rush. And I knew that was coming, so what I tried to do is meet with the companies and use the Defense Production Act to get a half a billion more tests and figure out how to get them to their homes, get them on the shelves in the store.

I mean, so that — that’s what it’s all about.

Yes?

Q Mr. President, what’s your message to Americans who are trying to get tested now and who are not able to get tested and who are wondering what took so long to ramp up testing?

THE PRESIDENT: Come on. What took so long?

Q That's what — I'm hearing that from people who are trying to get tested now before the holidays.

THE PRESIDENT: Well, what took so long is — it didn't take long at all. What happened was the Omicron virus spread even more rapidly than anybody thought.

If I had told you four weeks ago that this would spread by — a day-to-day basis it would spread by 50, 100 percent, 200 percent, 500 percent, I think you would have looked at me and say, "Biden, what are you drinking?" But that's what it did.

Now, we don't know what's going to happen from here. It looks — there's some evidence that, in South Africa where a lot of this started, that it's dropping off quickly, too. We don't know.

But I do know that we're not going to be in a position, like I said when we — remember we were having a problem with masks and gowns and the like? I said, "I promise you."

Remember the critici- — I got questions from some of you. "Why are you still paying for all these masks and gowns? Why you stockpiling this?" Because we don't know. It turns out we're going to need them.

In the back, and then —

Q Do travel bans work, sir, and will you reverse the travel ban now that Omicron is so prevalent here in the U.S.?

THE PRESIDENT: I'm considering reversing. I'm going to talk with my team in the next couple of days.

Look, remember why I said we put the travel ban on: It's to see how much time we had before it hit here so we could begin to decide what we needed by looking at what's happening in other countries.

And — but we're past that now. And so, it's something that is being raised with me by the docs, and I'll have an answer for that soon.

Q Mr. President, you often talk about the importance of keeping your word of trust. Do you believe Senator Manchin kept his word to you? And how do you rebuild trust with progressives in your party to advance your legislation now?

THE PRESIDENT: You know, I told you before — you’ve heard me say this before: Some people think maybe I’m not Irish because I don’t hold a grudge.

Look, I want to get things done. I still think there’s a possibility of getting Build Back Better done.

What I don’t want to do is get into — and Joe went on TV today and — I don’t know if it was TV or not; I’m told he was speaking to the liberal caucus in the House and said, “Joe Biden didn’t mislead you, I misled you.”

And so, look, I’m not — I’m not looking for — let me say something: You saw what happened yesterday. All the talk about how my Build Back Better plan was going to increase inflation, was going to cause these debts and all the like — what happened?

Goldman Sachs and others said if we don’t pass Build Back Better, we’re in trouble — because it’s going to grow the economy. And without it, we’re not going to grow.

And what happened? Stock prices went way down. It took a real dip.

If you take a look, the va- — I wasn’t — everybody thinks because I quoted 17 Nobel laureates saying, “This is going to help inflation” — think about it in terms of if you’re a hardworking person and you’re making 60 grand if you’re alone, if you’re mom or just on her own; or if you’re making 80 grand — a mom and dad, 90 grand, like a lot of people do, and you’re worried about inflation: You should be worried about it because it’s a devastating thing for people who are working class and middle-class folks. It really hurts.

Where is most of the cost now? The cost is finding it in gasoline, even though I’ve put — even though I was able to bring it down 12 cents a gallon and will come down more, I believe. We talked about what the cost in food prices going up, et cetera.

But look what’s in — look what’s in Build Back Better: Childcare — you can reduce it by up to 70 percent. That will be the difference between 20 million women who go — aren’t back in the workforce being able to go back, if you pass it.

We’re talking about — we’re talking about healthcare, insulin. We’re in a situa- — we got — we got 200,000 kids with Type 1 diabetes. You know what it’s costing? It cost somewhere between 10 cents and 10 dollars to come up with a formula — okay? — a while ago. All right?

You know what it's costing on average? \$560, \$640 a month, up to \$1,000 a month.

What do you do if you're a mom and a dad working with minimum wage, busting your neck, and you look at your kid and you know if you don't get that vaccine for them — I mean, that — excuse me — if you don't get that drug for them, if you don't get that — that — that — be able to take that, what happens? They're like to go into a coma and maybe die.

Not only do you put the kid's life at stake, you strip away all the dignity of a parent looking at their child. I'm not joking about this.

Imagine being a parent, looking at a child, and you can't afford — you have no house to borrow against, you have no savings. It's wrong. But all the things in that bill are going to reduce prices and cost for middle-class and working-class people. It's going to reduce their costs.

What's inflation? Having to pay more than the money you have because things have gone up. Well, it'll bring down all those costs across the board, from childcare to a Child Care Tax Credit.

But I'm not supposed to be having this press conference right now.

Q Mr. President, did Senator Manchin break his commitment to you? When you announced the framework, the White House says that all 50 senators were believed to get behind it — all 50 Democratic senators. So, did Senator Manchin break his commitment to you?

THE PRESIDENT: Senator Manchin and I are going to get something done. Thank you.

3:11 P.M. EST

DEFENDANTS' EXHIBIT 157:

IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA

The State of Missouri, *et al.*,

Plaintiffs,

v.

President Joseph R. Biden, Jr., in his official
capacity as President of the United States of
America, *et al.*,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF LARISSA L. KNAPP
FEDERAL BUREAU OF INVESTIGATION

I, Larissa L. Knapp, hereby declare as follows, pursuant to 28 U.S.C. § 1746:

1. I am the Executive Assistant Director (EAD) of the National Security Branch (NSB) of the Federal Bureau of Investigation (FBI) in Washington, D.C. I have held this position since May 2022. As EAD of NSB, I oversee all national security investigative and intelligence operations, including counterintelligence, counterterrorism, and weapons of mass destruction cases, as well as the Terrorist Screening Center
2. Prior to becoming EAD of NSB, I was EAD of the FBI's Human Resources Branch, which includes the Human Resources, Security, and Training Divisions. While serving as EAD of the Human Resources Branch, I also led the FBI's business functions as the acting Associate Deputy Director. Prior to that, I served in various supervisory capacities in the FBI's Security Division, the Washington Field Office, the Directorate of Intelligence, and the Counterterrorism Division. I began my FBI career in 1997 as a Special Agent in the

New York Field Office, where I investigated criminal computer intrusion and intellectual property matters. In 2003, I transferred to the U.S. Virgin Islands to work multiple threats, including counterterrorism and criminal cases.

2. The statements contained in this declaration are based upon my personal knowledge, my background, training, and experience related to FBI investigations and operations, and my review and consideration of documents and information available to me in my official capacity.
3. Through the performance of my official duties, I have been advised of this civil action, in which Plaintiffs allege that the Biden Administration and various government agencies and officials pressure or coerce social media companies into censoring viewpoints and speakers that Defendants disfavor. I understand that the operative complaint in this matter includes the FBI and two FBI officials as defendants, along with numerous other government agencies and officials, and that the allegations concerning the FBI and FBI officials focus on the FBI's Foreign Influence Task Force.
4. I am advised that Plaintiffs have filed a Motion for Preliminary Injunction ("PI") that would apply to the FBI and certain other named defendants. I am submitting this declaration in support of the Government's memorandum of law in opposition to the PI motion, to address the impact of the proposed PI on the FBI's ability to carry out its national security and law enforcement missions.¹
5. I am advised that Plaintiffs make the following request regarding the scope of a PI:

The Court should enter a preliminary injunction preventing Defendants, and their agents, officers, employees, contractors and all those acting in concert with them, from taking any steps to demand, urge, encourage, pressure, coerce, deceive,

¹ This declaration only addresses the proposed PI's impact on the FBI's ability to carry out its missions. It does not attempt to address Plaintiffs' specific allegations regarding the FBI or its personnel.

collude with, or otherwise induce any social-media company or platform for online speech, or any employee, officer, or agent of any such company or platform, to censor, suppress, remove, de-platform, suspend, shadow-ban, de-boost, deamplify, issue strikes against, restrict access to, demonetize, or take any similar adverse action against any speaker, content, or viewpoint expressed on social media. The Court should also preliminarily enjoin Defendants from acting in concert with any others, including but not limited to persons and entities associated with the Center for Internet Security, the Election Integrity Partnership, and the Virality Project, to engage in the aforementioned conduct, and from acting in concert with any such others who are engaged in any of the aforementioned conduct.

As explained below, there is a range of situations—some of which are completely unrelated to the allegations against the FBI and FBI officials in this lawsuit—in which it would be in the public interest and consistent with the FBI’s law enforcement and national security missions for the FBI to notify a social media platform of criminal conduct, national security threats, or other threats on its platform. Thus, the Russian, Chinese, and Iranian governments, other foreign malign actors individuals or groups intent on preventing qualified voters from voting, terrorists, cyber criminals, individuals or groups involved in crimes against children, and a wide variety of other criminals would benefit, and the American public and victims of crime would be harmed, if the Court were to issue the proposed PI and if it were interpreted to prevent the FBI from communicating with social media platforms about criminal conduct, national security threats, and other threats on their platforms.

THE FBI’S ROLES AND RESPONSIBILITIES

6. The FBI’s mission is to protect the American people and uphold the Constitution of the United States. In carrying out that mission, the FBI defends the United States against terrorist and foreign intelligence threats, upholds and enforces the criminal laws of the United States, provides leadership and criminal justice services to federal, state, municipal,

and international agencies and partners, and engages in outreach and information-sharing with private sector entities. In order to defend the country from a range of national security and major criminal threats, the FBI uses an intelligence-driven and threat-focused approach, combining its investigative and intelligence operations to be more analytical and preventative, more aware of emerging threats, and better able to stop them before they turn into crimes, including acts of terrorism.

7. The FBI's top priority is protecting the United States from terrorist attacks. In carrying out the FBI's paramount mission of securing the nation from terrorism, criminal prosecution is just one of several means that the FBI uses to protect national security. Working closely with its partners, the FBI uses its investigative and intelligence capabilities to neutralize terrorist cells and operatives in the United States, to help dismantle extremist networks worldwide, and to cut off financing and other forms of support provided by terrorist sympathizers.
8. The FBI's second highest priority is to protect the United States against foreign intelligence, espionage, and cyber operations, and it has been given broad authorities in these areas that encompass both its law enforcement and counterintelligence responsibilities. Specifically, the FBI is the primary investigative agency of the federal government and is authorized to investigate all violations of federal laws that are not exclusively assigned to another agency.² The FBI has also been specifically designated to

² See 28 U.S.C. § 533, which provides that the Attorney General may appoint officials to, *inter alia*, detect crimes against the United States and to conduct such other investigations regarding official matters under the control of the Department of Justice and the Department of State as may be directed by the Attorney General. The Attorney General Guidelines on Domestic FBI Operations, found at <https://www.justice.gov/archive/opa/docs/guidelines.pdf>, states at p. 5 that as the primary investigative agency of the federal government, the FBI "has the authority and responsibility to investigate all violations of federal law that are not exclusively assigned to another federal agency. The FBI is further vested by law and by Presidential directives with the primary role of carrying out investigations within the United States of threats to the national security. This includes the lead domestic role in investigating terrorist threats

take charge of investigative work in matters relating to espionage, sabotage, subversive activities, and related matters.³ In addition, Executive Order 12333, as amended, establishes the FBI as the lead counterintelligence agency within the United States, and authorizes the FBI to conduct counterintelligence activities and collect, analyze, produce, and disseminate foreign intelligence and counterintelligence to support national and departmental missions.⁴

9. The FBI's remaining mission priorities include cyber crime, public corruption, civil rights, transnational criminal enterprises, white collar crime, and violent crime. Various federal statutes authorize the FBI to conduct investigations of federal crimes, make seizures and arrests, and serve warrants, both under national security authorities (title 50 of the U.S. Code) and law enforcement authorities (title 18 of the U.S. Code). For example, as relevant here, except with respect to certain offenses affecting the duties of the United States Secret Service, the FBI has primary investigative authority for all computer network intrusions relating to threats to the national security, including "cases involving espionage, foreign counterintelligence, [and] information protected against unauthorized disclosure for reasons of national defense or foreign relations . . ."⁵

EFFORTS TO COUNTER FOREIGN MALIGN INFLUENCE OPERATIONS

10. The United States is confronting multifaceted foreign threats seeking to influence our political, economic or national security conditions through subversive, undeclared,

to the United States, and in conducting counterintelligence activities to meet foreign entities' espionage and intelligence efforts directed against the United States."

³ 28 C.F.R. § 0.85(d).

⁴ See Executive Order 12333, as amended, § 1.7(g).

⁵ 18 U.S.C. § 1030(d)(2).

coercive, and criminal actions. Such foreign malign influence operations include foreign government attempts to sway U.S. voters' preferences and perspectives, shift U.S. policies, increase discord in the United States, and undermine the American people's confidence in our democratic institutions and processes.

11. Foreign malign influence is not a new problem. As stated in the July 2018 Report of the Attorney General's Cyber-Digital Task Force:⁶

Hostile foreign actors have long sought to influence, and subvert, our Nation's democratic institutions. Modern technology—including the Internet and social media platforms—has both empowered and emboldened foreign governments and their agents in their attempts to affect U.S. attitudes, behaviors, and decisions in new and troubling ways. . . . Foreign influence operations include covert actions by foreign governments intended to sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives. Foreign influence operations can pose a threat to national security—and they can violate federal criminal law.

12. Russia, the People's Republic of China (PRC), and Iran are the most active in foreign malign influence operations aimed at the United States. According to the Mueller Report,⁷ the first form of Russian election influence came principally from a Russian organization called the Internet Research Agency, LLC (IRA), funded by Yevgeniy Viktorovich Prigozhin and companies he controlled:

The IRA conducted social media operations targeted at large U.S. audiences with the goal of sowing discord in the U.S. political system. . . . The IRA and its employees began operations targeting the United States as early as 2014. Using fictitious U.S. persons, IRA employees operated social media accounts and group pages designed to attract U.S. audiences. These groups and accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled

⁶ Found at <https://www.justice.gov/archives/ag/page/file/1076696/download>. A July 2, 2018, letter from then-Deputy Attorney General Rod J. Rosenstein to then-Attorney General Jefferson B. Sessions III, which prefaces the Cyber-Digital Task Force report, states that in February 2018, Attorney General Sessions directed the formation of a Cyber-Digital Task Force to “undertake a comprehensive assessment of the Department’s work in the cyber areas, and to identify how federal law enforcement can even more effectively accomplish its mission in this vital area.”

⁷ Special Counsel Robert S. Mueller, III’s March 2019 Report on the Investigation Into Russian Interference in the 2016 Presidential Election. Volume I of the Mueller Report is found at <https://www.justice.gov/archives/sco/file/1373816/download>.

by U.S. activists. . . . By the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts.

Mueller Report Vol I, at 14.⁸

13. Based on the FBI's national security and law enforcement responsibilities cited above, the FBI is the lead federal agency responsible for investigating foreign influence operations. In the fall of 2017, Director Christopher Wray established the Foreign Influence Task Force (FITF) to identify and counteract malign foreign influence operations targeting the United States. The FITF is led by the FBI's Counterintelligence Division and is composed of agents, analysts, and professional staff from the Counterintelligence, Cyber, Counterterrorism, and Criminal Investigative Divisions. It is specifically charged with identifying and combating foreign influence operations targeting democratic institutions and values inside the United States.
14. Initially, the FITF's efforts to combat foreign malign influence focused solely on the threat posed by Russia. Following the 2018 midterm elections, the FITF broadened its focus to confront malign foreign operations of the PRC, Iran, and other global adversaries. Currently, the PRC is at least as active as Russia in its malign foreign influence operations against the United States.
15. The FITF's work includes managing operations and field office investigations, and information and intelligence sharing with federal, state, and local government agencies, as well as with U.S. private sector entities. Specifically, with respect to U.S. social media platforms, the FBI, together with its Intelligence Community partners, may determine through investigation and intelligence gathering that an account that purports to be

⁸ On February 16, 2018, the IRA, Prigozhin, and others were indicted in connection with their operations to interfere with U.S. elections and political processes. See *United States v. Internet Research Agency LLC, et al.*, No.18-cr-00032 (D.D.C.).

controlled by a U.S. person is, in fact, controlled by a covert foreign malign actor. The operation of a social media account by a foreign malign actor under a false identity is typically a violation of a company's terms of service.⁹ In such cases, the FBI may share with social media companies the indicators or selectors regarding that account or that foreign actor, to include IP addresses, email accounts, social media accounts, website domain names, or file hash values, that will enable social media companies to conduct their own independent investigation into whether there is a violation of their terms of service. When that information is shared, it is the FBI's practice to convey to the company that the information is being shared for whatever action the company deems appropriate. The FBI's practice is to not pressure or coerce companies to take any action, and companies do not necessarily disclose to the FBI whether they took any action on a posting or account. But based on the information they do provide, sometimes they take action on a posting or account after receipt of information from the FBI and their own subsequent investigation, and sometimes they do not.¹⁰

16. A decision by the FITF to share information with a U.S. social media platform about a foreign malign actor's social media activity is not based upon the content or particular

⁹ It is my understanding that it may also be a violation of the Foreign Agents Registration Act, 22 U.S.C. § 611 et seq. or other criminal statutes depending on the circumstances, including, but not limited to: 18 U.S.C. § 371 (conspiracy); 18 U.S.C. § 1028A (aggravated identity theft); 18 U.S.C. § 951 (acting in the United States as an agent of a foreign government without prior notification to the Attorney General); 18 U.S.C. § 1030 (computer fraud and abuse); 18 U.S.C. §§ 1343, 1344 (wire fraud and bank fraud) and 52 U.S.C. §§ 30109, 30121 (soliciting or making foreign contributions to influence federal elections, or donations to influence state or local elections).

¹⁰ For examples of a social media platform's reporting on its enforcement of its terms of service, see Meta's November 13, 2018, report "More Information About Last Week's Takedowns" found at <https://about.fb.com/news/2018/11/last-weeks-takedowns/>; Twitter's October 8, 2020, blog "Disclosing networks to our state-linked information operations archive" found at https://blog.twitter.com/en_us/topics/company/2020/disclosing-removed-networks-to-our-archive-of-state-linked-information; and Meta's May 6, 2021, report "April 2021 Coordinated Inauthentic Behavior Report" found at <https://about.fb.com/news/2021/05/april-2021-coordinated-inauthentic-behavior-report/>.

viewpoint expressed in a posting but rather on the fact that the account is part of a *covert* effort by a *foreign* malign actor.

17. While the FBI is responsible for investigating violations of the Foreign Agents Registration Act (FARA), the FITF does not identify for U.S. social media companies postings by hostile foreign actors where the postings are not covert, regardless of the content. For example, the FITF would not identify for a U.S. social media platform a post or account overtly attributed to RT (formerly known as “Russia Today”), which is registered under FARA as an agent of a Russian government entity and maintains accounts on social media, including Facebook and Twitter.
18. The FITF’s efforts to combat foreign malign influence operations are consistent with the findings of the current and prior administrations regarding U.S. national security and foreign policy. On September 12, 2018, President Trump issued Executive Order 13848, which states that the President found “that the ability of persons located, in whole or substantial part, outside the United States to interfere in or undermine public confidence in United States elections including through the unauthorized accessing of election and campaign infrastructure or the covert distribution of propaganda and disinformation constitutes an unusual and extraordinary threat to the national security and foreign policy of the United States.” Based in part on this finding, the President declared a national emergency in accordance with section 202(d) of the National Emergencies Act, 50 U.S.C. § 1622(d), with respect to the threat of foreign interference in or undermining public confidence in United States elections. On September 10, 2019, and then again on September 10, 2020, President Trump found that this threat continued and therefore continued the national emergency he previously declared. President Biden also found that

this threat continues and therefore continued the national emergency declaration on September 7, 2021, and September 7, 2022.

19. Consistent with the findings by Presidents Trump and Biden, the media has reported that Yevgeniy Prigozhin—as previously noted, the primary funder of the IRA, who is charged with crimes relating to the IRA’s political and electoral interference operations in the United States—stated in 2022 that the Russians will continue to interfere in U.S. elections.¹¹
20. Thus, the Russian, PRC, and Iranian governments, and other foreign malign actors, would benefit, and the United States’ national security would be harmed, if the Court were to issue the proposed PI and if it were interpreted to prevent the FBI from notifying a social media company that a particular account on its platform is operated by a covert foreign malign actor. Such a ruling would serve as an open invitation for these foreign malign actors to step up their deceptive efforts to sow division within the United States, undermine our democratic processes and institutions, and steer policy and regulatory decisions in favor of their strategic objectives, and diminish our nation’s capacity to defend its interests on the world stage.

ELECTION-RELATED TIME, PLACE, AND MANNER DISINFORMATION

21. The U.S. Government and the American people have a compelling interest in maintaining the integrity of election procedures, and based on the authorities cited above, the FBI has been given responsibility to investigate three categories of federal election crimes:

¹¹ For example, see November 7, 2022, Associated Press article “Putin-linked businessman admits to US election meddling” found at <https://apnews.com/article/2022-midterm-elections-business-social-media-7fefa7ab0491b653f6094a4d090155fe>.

(1) voter/ballot fraud, (2) civil rights violations, and (3) campaign finance offenses. I understand that posting objectively false information on social media concerning the time, place, or manner of elections with the intent to prevent qualified voters from effectively voting may be a violation of 18 U.S.C. § 241, which makes it a crime to conspire to “injure” any person “in the free exercise or enjoyment of any right or privilege secured to him by the Constitution or the laws of the United States.”¹² For this reason, separate from the work of the FITF, the FBI and the DOJ work to counter efforts to prevent qualified voters from effectively voting by deceiving them as to the time, place, or manner of an election.

22. Specifically, in the days immediately preceding a presidential or mid-term election, and on election day itself, the FBI stands up “command posts” at FBI Headquarters and in its field offices across the country. The command posts in the field offices are staffed by FBI Special Agents, analysts, and support personnel, as is the command post at FBI Headquarters, but the latter is also staffed by attorneys from DOJ and the FBI Office of the General Counsel. The command posts facilitate the FBI’s and DOJ’s ability to address federal election crimes, including but not limited to civil rights violations, which may be occurring.

23. If an FBI field office is notified—for example, by a state election official—of a posting on a social media platform which contains objectively false information about the time, place, or manner of an election, the field office will conduct an initial review as to whether the posting appears to constitute a violation of 18 U.S.C. § 241 or evidence of such a violation. If so, the field office will relay the information to the FBI Headquarters

¹² See January 23, 2023, Memorandum and Order denying defendant’s motion to dismiss the indictment in *United States v. Douglass Mackey*, No. 21-cr-00080 (E.D. N.Y.), ECF No. 54.

command post, and the FBI and DOJ personnel at the command post will review the report and determine whether the posting appears to constitute a violation of 18 U.S.C. § 241 or evidence of such a violation. If it does, the report is passed to the FBI's San Francisco Division command post, which then relays the information to the social media platform.¹³ This relaying is done in an effort to minimize victimization where possible, rather than rely solely on potential prosecution as a means to protect the public. Again, the FBI does not pressure or coerce platforms into taking any action, but rather relies on the platforms to take whatever action they deem appropriate in light of their terms of service.

24. Thus, individuals or groups intent on deceiving U.S. citizens about the time, place, or manner of elections would benefit, and the public would be harmed, if the Court issues the proposed PI and if the PI were interpreted to prevent the FBI from sharing that information with social media platforms.

TERRORISTS USING SOCIAL MEDIA PLATFORMS

25. As noted above, preventing terrorist attacks remains the FBI's top priority. The FBI remains concerned that foreign terrorist organizations, such as Islamic State of Iraq and ash-Sham (ISIS) and al Qaeda and their affiliates, intend to carry out or inspire large-scale attacks in the United States.
26. Many terrorist organizations use various digital communication platforms, including social media, to reach individuals they believe may be susceptible and sympathetic to violent terrorist messages. Terrorists in ungoverned spaces—both physical and virtual—readily

¹³ Because most social media platforms are headquartered within the San Francisco Division's geographic area of responsibility, the San Francisco Division is the FBI's primary point of contact with social media platforms regarding election time, place, or manner disinformation.

disseminate propaganda and training materials to attract easily influenced individuals around the world to their cause. With the broad distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable persons of all ages across the globe. These efforts are not new—see the attached September 21, 2012, letter from members of Congress to then-FBI Director Mueller about foreign terrorist organizations using Twitter to further their jihadist agendas.¹⁴

27. No group has been as successful at drawing people into its perverse ideology as ISIS, which has proven dangerously competent at employing such tools. Despite its loss of physical territory in Iraq and Syria, ISIS remains relentless in its campaign of violence against the United States and our partners. ISIS uses traditional media platforms as well as widespread social media campaigns to propagate its ideology. Like other foreign terrorist groups, ISIS advocates for lone offender attacks in the United States and Western countries via videos and other English language propaganda that have, at times, specifically advocated for attacks against civilians, the military, law enforcement, and intelligence community personnel.
28. ISIS and its supporters continue to aggressively promote its hate-fueled rhetoric and attract like-minded violent extremists with a willingness to conduct attacks against the United States and our interests abroad. The message is not tailored solely to those who overtly express signs of radicalization. It is seen by many who use messaging applications and participate in social networks.
29. Al Qaeda maintains its desire to both conduct and inspire large-scale, spectacular attacks. Because continued pressure has degraded some of the group's senior leadership, the FBI

¹⁴ The September 21, 2012, letter is attached hereto as Exhibit 1.

assesses that, in the near term, al Qaeda is more likely to continue to focus on cultivating its international affiliates and supporting small-scale, readily achievable attacks in regions such as East and West Africa. Propaganda from al Qaeda leaders continues to seek to inspire individuals to conduct their own attacks in the United States and other Western nations.

30. Promotion or facilitation of terrorist activity is typically a violation of a social media platform's terms of service. Therefore, in some circumstances, the FBI provides social media platforms with notice, for whatever action they deem appropriate, that foreign terrorists or those promoting terrorism are using their platforms.¹⁵ The FBI's practice is to not pressure or coerce companies to take any action, and companies do not necessarily disclose to the FBI whether they took any action on a posting or account. However, the FBI's experience is that social media companies share the FBI's and the general public's interest in combatting terrorism and therefore will often (but not always) enforce their terms of service to prevent this activity on their platforms. By way of example, in a February 5, 2016, blog post, Twitter reported that since the middle of 2015, they had suspended over 125,000 accounts for threatening or promoting terrorist acts, primarily related to ISIS.¹⁶

31. Thus, ISIS, al Qaeda, and other terrorist groups who use social media to promote their agendas would benefit, and the risk to the American public from terrorism would

¹⁵ The FBI may learn of this activity through its national security investigations, from other members of the U.S. Intelligence Community, through foreign partners, or by other means. Social media activity by foreign terrorist organizations may or may not constitute a crime under U.S. law and may or may not be readily accessible to people in the United States—some U.S. social media platforms, like Facebook, are popular across the globe and foreign terrorist organizations or supporters may create Facebook groups in which they post terrorist propaganda in their native languages.

¹⁶ See https://blog.twitter.com/en_us/a/2016/combating-violent-extremism.

increase, if the proposed PI were issued and interpreted to prevent the FBI from notifying social media platforms of terrorist groups' activity on those platforms.

CYBER CRIMINAL ACTIVITY ON SOCIAL MEDIA PLATFORMS

32. Malicious cyber activity threatens the public's safety and our national and economic security, and over recent years, the FBI has seen a wider-than-ever range of cyber actors threaten Americans' safety, security, and confidence in our digitally connected world. Cyber-criminal syndicates and nation-states keep innovating ways to compromise our networks and maximize the reach and impact of their operations, such as by selling malware as a service or by targeting vendors to access scores of victims by hacking just one provider.
33. The FBI's cyber strategy is to impose risks and consequences on cyber adversaries. Our goal is to change the behavior of criminals and nation-states who believe they can compromise U.S. networks, steal financial and intellectual property, and put critical infrastructure at risk without facing risk themselves. To do this, we use our unique mix of authorities, capabilities, and partnerships to impose consequences on our cyber adversaries.
34. The FBI is the lead federal agency for investigating cyber attacks and intrusions. We collect and share intelligence and engage with victims while working to unmask those committing malicious cyber activities.
35. Social media platforms are frequently used by cyber criminals to commit crimes. For example, platforms typically provide for some type of direct messaging to users, which cyber criminals can use to conduct spear phishing attacks. Spear phishers target select groups of people with something in common—for example, they work at the same

company, bank at the same financial institution, attend the same college, or order merchandise from the same website. Using inside information that may have been obtained through hacking or by combing through websites, blogs, or social media platforms, cyber criminals send messages through the social media platform that look like the real thing to targeted victims, offering urgent and legitimate-sounding explanations as to why they need the victim's personal data. Victims are asked to click on a link inside the message that takes them to a phony but realistic-looking website, where they are asked to provide passwords, account numbers, user IDs, access codes, PINs, and alike. Once criminals have the victim's personal data, they can access their bank account, use their credit cards, and create a whole new identity using their information. Spear phishing can also trick the victim into downloading malicious codes or malware after they click on a link embedded in a message, which is an especially useful tool in crimes like economic espionage where sensitive internal communications can be accessed, and trade secrets stolen. Malware can also hijack the victim's computer.

36. Social media is also a ripe platform for "malvertizing," in which cyber criminals post advertisements on social media that either link to fake login pages to steal credentials or have advertisements that end up linking to other pages that deceive victims into downloading malware.
37. As part of the FBI's effort to combat cyber crime, the FBI may in some circumstances notify social media platforms of spear phishing, malvertizing, or other fraud enabling activities on their platforms. These notifications may be about general trends that the FBI is seeing or about particular incidents. The FBI's practice is to not pressure or coerce companies to take any actions, and companies do not necessarily disclose to the FBI

whether they took any action on such fraud. In addition, the FBI has on occasion been contacted by companies when their social media accounts have been taken over by cyber criminals or when cyber criminals have established fraudulent accounts which appear to be operated by those companies and the companies have been unsuccessful in reaching the social media platforms directly to report the incident. On occasion, the FBI has relayed the incident to the social media platform.

38. Thus, cyber criminals who use social media platforms to commit their crimes would benefit, and the public would be placed at greater risk from cybercrime, if the Court were to issue the proposed PI and if it were interpreted to prevent the FBI from communicating with social media platforms about cyber criminal activity on their platforms.

CRIMES AGAINST CHILDREN ON SOCIAL MEDIA PLATFORMS

39. The FBI plays an important role in the effort to prevent violent crimes against children, to include contact offenses against children (production of child sexual abuse material (CSAM),¹⁷ sextortion, domestic travel to engage in sexual activity with children, and international travel to engage in sexual activity with children); sexual exploitation of children (online networks and enterprises manufacturing, trading, distributing, and/or selling CSAM); and trafficking of CSAM (distribution or possession). Social media is a major forum for criminals to engage in the heinous sexual exploitation of children and the trafficking of CSAM, and federal law requires electronic service providers, including social

¹⁷ The FBI and other entities involved in the prevention of violent crimes against children now use the term “child sexual abuse material” instead of “child pornography.”

media platforms, to report certain online child sexual exploitation once the provider obtains actual knowledge of the facts or circumstances.¹⁸

40. The mission of the FBI's Crimes Against Children program is to (1) provide a rapid, proactive, and comprehensive ability to counter all threats of abuse and exploitation to children when those crimes fall under the authority of the FBI; (2) identify, locate, and recover child victims; and (3) strengthen relationships between the FBI and federal, state, local, tribal, and international law enforcement partners to identify, prioritize, investigate, and deter individuals and criminal networks exploiting children.
41. The FBI also works closely with the National Center for Missing & Exploited Children (NCMEC). NCMEC's CyberTipline receives reports of child sexual exploitation incidents via an online form and maintains a 24-hour hotline. FBI personnel assigned to the NCMEC review information that is provided to NCMEC's tip line and work to identify individuals suspected of any of the following: possession, manufacture or distribution of CSAM; online enticement of children for sexual acts; child sexual tourism; or other sexual exploitation of children. Once a potential suspect has been identified, investigators compile information and forward it to the appropriate FBI field office for investigation.
42. As is indicated on NCMEC's website,¹⁹ NCMEC works closely with electronic service providers, including social media platforms, on voluntary initiatives that many companies choose to engage in to deter and prevent the proliferation of online child sexual exploitation

¹⁸ See 18 U.S.C. § 2258A (reporting requirements of providers) and 2258E(6)(defining "provider" for purposes of sections 2258A through 2258E).

¹⁹ <https://www.missingkids.org/theissues/csam>.

images. Companies also receive notices from NCMEC about suspected CSAM on their servers.²⁰

43. The proposed PI's prohibition on "acting in concert with others" could potentially prevent NCMEC from working with the FBI to keep CSAM and other crimes against children from taking place on social media platforms. In addition, although the FBI does not routinely contact social media platforms directly to flag CSAM and other crimes against children on their platforms, there are situations where that would be warranted in order to prevent imminent or ongoing harm to children. For example, notification to the platform would be warranted if the FBI were aware of live streaming of sexual abuse of a child, a particular user in a chat room grooming children for exploitation, or a particular user committing ongoing sexploitation crimes against children.²¹
44. The proposed PI could potentially prevent NCMEC and the FBI from alerting a social media platform of CSAM or other crimes against children taking place on its platform. Thus, individuals involved in the production and dissemination of CSAM or involved in other heinous crimes against children taking place on social media would benefit, and children would be placed at greater risk of becoming their victims, if the Court were to issue the proposed PI, and if it were interpreted to apply to the FBI's efforts to prevent crimes against children.

²⁰ Pursuant to 18 U.S.C. § 2258C(a), NCMEC may provide certain information relating to any CyberTipline report, such as hash values or other unique identifiers associated with a specific visual depiction, to a provider in order to permit that provider to stop the online sexual exploitation of children.

²¹ In addition, 18 U.S.C. § 2258B(c)(2) requires providers to destroy CSAM images "upon a request from a law enforcement agency."

OTHER CRIMES AND SECURITY THREATS ON SOCIAL MEDIA PLATFORMS

45. In addition to the contexts discussed above, there may be other situations where it would be in the public interest for the FBI to notify a social media platform of criminal conduct or security threats on its platform.
46. For example, if properly classified national security information is illegally posted on a social media account and foreign adversaries become aware of it, that posting would reasonably be expected to cause some level of damage to national security.²² In such a situation, I expect that the FBI would ask the social media platform to remove the information.²³ There has also been public reporting that some foreign intelligence services use certain job networking platforms to recruit former government employees to provide classified information,²⁴ so in some circumstances it may be in the interests of national security for the FBI to notify a platform of that activity. There have also been cases where individuals have posted explicit threats against FBI personnel on social media or posted personal information of FBI personnel and federal judges in order to encourage violence against those individuals. In some circumstances, the FBI has asked platforms to take down

²² Under Executive Order 13526, section 1.2(a), the unauthorized disclosure of Top Secret information is reasonably expected to cause exceptionally grave damage to the national security; unauthorized disclosure of Secret information is reasonably expected to cause serious damage to the national security; and unauthorized disclosure of Confidential information is reasonably expected to cause damage to the national security.

²³ That situation did occur with respect to posting on Twitter, and Twitter removed the posting at the FBI's request. See Government's Sentencing Position, ECF NO. 47, in *United States v. James Robert Schweitzer*, No. SA CR 20-188-JLS (C.D. Cal.), attached hereto as Exhibit 2.

²⁴ See April 4, 2019, NBC News article titled "How a \$230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China" found at <https://www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691>.

those postings.²⁵ A situation could also arise where the FBI might notify a social media platform that the sale of dangerous illegal drugs is taking place on the platform.

47. These are just examples. Given the broad scope of the FBI's national security and law enforcement missions, the wide range of activity taking place on social media, and the constantly emerging threats from criminals, foreign adversaries, and other hostile actors, it is not possible to predict all the situations that could arise that might prompt the FBI to notify social media platforms of criminal activity or security threats on their platforms. The terms of the proposed PI appear to be expansive in scope and to lack clear boundaries. It makes no exception for situations involving criminal activity or security threats on social media platforms, and appears to go far beyond enjoining efforts to unlawfully "pressure" or "coerce" social media platforms to take action. Thus, it would create a dangerous situation in which the FBI may not be able to communicate with social media platforms in order to protect the national security and targets of crime and security threats.

PRIVATE SECTOR OUTREACH AND INFORMATION SHARING

48. As previously noted, the FBI's approach to its law enforcement and national security mission is to prevent crimes and mitigate national security threats, where possible, before they do damage. A critical part of that approach is for the FBI to work with the private sector to enhance the FBI's understanding of the risks it confronts and its needs, and to furnish the private sector with information that will help it, and the people who depend on

²⁵ According to media reports, a similar situation recently occurred with respect to police officers with the Los Angeles Police Department. An individual posted photographs and other information about LAPD officers on a website and offered bounties for the killing of officers. The website was apparently posted on Twitter, and Twitter took down the posting at the request of the police union. See <https://abc7.com/twitter-killercops-account-suspended-los-angeles-police-union-lapd/13031738/>.

the services the private sector offers, to avoid becoming victims. With respect to social media platforms, the FBI on occasion provides the platforms with information about general trends in criminal activity or national security threats that might impact their platforms. For example, with respect to cyber crime, the FBI works hard to push important threat information to network defenders. The FBI also shares information about trends in disinformation operations by covert foreign malign actors, and about code words and symbols being used by terrorist groups on social media. The proposed PI is so vague and broad that it could raise a question whether that kind of outreach and information sharing would be covered under the PI, even if no particular social media posting is being flagged.

49. The proposed PI is so vague and broad that it might also be construed to cover general statements by FBI personnel—not necessarily even direct communications between the FBI and social media platforms—about trends in criminal activity. For example, if a social media platform becomes aware of congressional testimony by an FBI official that there are increasing reports of certain types of cyber crime, that certain terrorist organizations are becoming more active, or that crimes against children continue to be a serious problem, that might be regarded as “encouraging” the platform to be more proactive in policing its platform for terms of service violations. Viewed that way, the FBI could not make any statements or take any action that might influence or “encourage” social media platforms to protect their business and their users from criminal conduct or other conduct that violates their terms of service.

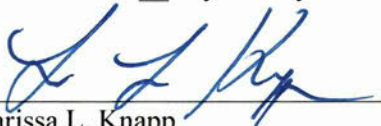
CONCLUSION

50. As stated above, the FBI’s national security and law enforcement missions include not only the investigation of crimes or threats that have already been carried out, but the prevention

of crimes and the protection of intended victims. Moreover, in the context of national security threats and criminal conduct by agents of foreign governments or by other foreign actors, those foreign actors may view themselves as beyond the reach of federal prosecutors, and so the threat of criminal prosecution may be not an effective deterrent. In those and other circumstances, the FBI's law enforcement and national security efforts are most effectively aimed at preventing the criminal conduct or mitigating the national security threat, and this may involve notifying social media platforms of criminal conduct and security threats on their platforms. Thus, to the extent it is applied to the FBI, the proposed PI would be contrary to the interests of the national security, the American public, and victims of crime. Rather, it would benefit the Russian, PRC, and Iranian governments, other foreign malign actors, individuals or groups intent on preventing qualified voters from voting, terrorists, cyber criminals, individuals and groups involved in crimes against children, and a wide variety of other criminals. For the foregoing reasons, I urge the Court to deny the request for a PI with respect to the FBI or any FBI officials.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed this 1 day of May 2023



Larissa L. Knapp
Executive Assistant Director
National Security Branch
Federal Bureau of Investigation

EXHIBIT 1



Congress of the United States
House of Representatives
Washington, DC 20515-4302

September 21, 2012

Robert S. Mueller, III
Director, Federal Bureau of Investigations
935 Pennsylvania Avenue, NW
Washington, D.C. 20535-0001

Dear Director Mueller:

We are writing to express our concern about designated Foreign Terrorist Organizations' (FTOs) use of Twitter to further their jihadist agendas.

Designated FTOs like Al-Shabaab (@HSMPress), Hamas (@hamasinfo, @AlqassamBrigade, and @AqsaTVChannel) and Hezbollah (@almanarnews) all have active Twitter handles and use Twitter to recruit members, disseminate their message and encourage violent acts.

On February 26, 2008, the U.S. government, pursuant to Section 1(b) of Executive Order 13224, designated the Somali al-Qaeda affiliate Al-Shabaab as a Specially Designated Global Terrorist entity. Al-Shabaab is responsible for killing nearly 80 people in a series of suicide bombings in Kampala, Uganda during the 2010 World Cup and is currently leading the insurrection in Somalia that has killed thousands and displaced millions. On December 7, 2011, under the title "HSM Press – Harakat Al-Shabaab Al Mujahideen Press Office," and with an avatar of the Al-Qaeda flag, Shabaab opened a Twitter account (@HSMPress). One of its first tweets was, "The Jihad being waged here in Somali shall continue until the country is purified of all invaders." On June 16, 2012, it tweeted, "Praise be to Allah that slavishly obedient American lapdogs are increasingly joining the long list of the damned in the Arabian Peninsula." And, on May 22 2012, it tweeted, "May Allah grant victory to the Mujahideen throughout the Jihadi fronts." On Aug 8 2012, it tweeted, "The ambitions of the Mujahideen are unequivocally expressed; establish the Rule of Allah or attain martyrdom in its pursuit!" As of August 6, 2012, Shabaab had 13,869 followers and made over 700 tweets.

Since Hamas, designated as an FTO back in April 1993, sent its first tweet on November 21, 2009, it has posted a total of over 9,220 tweets in its various accounts, and it has gained over 19,036 followers. The accounts include those of Hamas Info, the main organization's office; Hamas' military arm, Izz Al-Din Al-Qassam Brigades; Hamas' media wing Al-Aqsa TV; Hamas' Political Bureau deputy chairman Moussa Abu Marzouq; Izzat Rishq, a senior Hamas official based in Syria; and Hamas Radio. So far, Hamas' tweets have included excerpts from the Koran to incite jihad and martyrdom attacks, links to YouTube videos inciting violence, and even calls for "a new Holocaust." One tweet touted how many "Zionist soldiers" Hamas killed, while another called for abducting Israelis.

A year after the Department of State designated Hezbollah itself as an FTO, it named Al-Manar a Specially Designated Global Terrorist entity and declared that it was "owned or controlled by the Iran-funded Hezbollah terrorist network," while the Department of Treasury, cited Al-Manar as "the media arm of Hezbollah." Al-Manar opened its Twitter account last November and, as of August 6, 2012, Al-Manar had tweeted an average of 250 tweets per day and had 18,903 followers. It is evident that Hezbollah understands the value of Twitter when it comes to spreading its propaganda.


FTO use of Twitter to encourage violence or to recruit others in furtherance of terrorism is not protected by free speech rights. As the Supreme Court decided in *Holder v. Humanitarian Law Project*, the material-support statute (18 U.S.C. Sections 2339A and 2339B) does not violate the freedom of speech guaranteed by the First Amendment. In fact, in that case, the plaintiffs wished to advance "only the legitimate activities of" two designated terrorist groups. In the instances raised above, we have examples of U.S. government-designated terrorist groups themselves specifically promoting their illegitimate activities. Therefore, it is clear that they too would fall under the Supreme Court's standard of "part of a broader strategy to promote terrorism" and thus not be afforded the protections of the U.S. Constitution.

The *Holder* decision has been complied with by other companies in the social media sphere, such as YouTube and Facebook, who have created policies to protect the public. YouTube's policy is centered on the flagging of terrorist videos. Users concerned about the content of a video can flag it under the category of "promotes hatred or violence against a protected group". YouTube then reviews the flag designation and takes the video down if the flag designation is accurate. Facebook's policy is based on rule of law and self-governance. It states, "In addition to using the State and Treasury Department lists, and the fact that our SRR (Statement of Rights and Responsibilities) prohibits anyone on those terrorist lists from using our service, we are also proactive in screening for those names and organizations. Our internal systems also employ keyword searches related to associated terminology." Just last month, Facebook removed a number of Hezbollah pages after both Google and Apple removed Hezbollah's applications from their stores.

The Federal Bureau of Investigation (FBI) is the arm of the government entrusted with the authority to take down Twitter accounts held by terrorists. Twitter maintains that it will take down any account requested by the FBI. However, as of the writing of this letter, the FBI has not made a single request to Twitter to take an account down. Meanwhile, U.S. designated terrorists continue to use an American company to spread its propaganda to the world, encouraging violence and garnering new recruits to continue the cycle of violence that kills innocent civilians around the world.

We respectfully ask for the FBI to reconsider its policy regarding Twitter accounts and use the tools that Congress has granted it in order to halt the spread of terrorist propaganda and to try to limit the expansions of these organizations. We look forward to receiving your response.

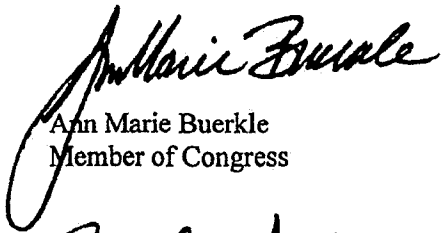
Sincerely,



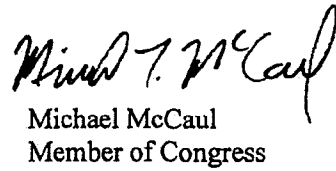
Ted Poe
Member of Congress



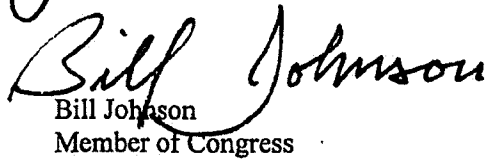
Bob Turner
Member of Congress



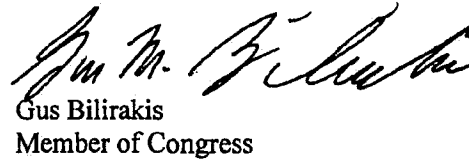
Ann Marie Buerkle
Member of Congress



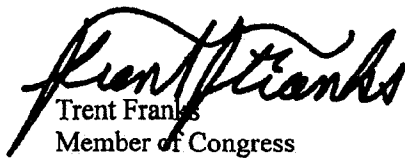
Michael McCaul
Member of Congress



Bill Johnson
Member of Congress



Gus Bilirakis
Member of Congress



Trent Franks
Member of Congress

EXHIBIT 2

1 TRACY L. WILKISON
Acting United States Attorney
2 CHRISTOPHER D. GRIGG
Assistant United States Attorney
3 Chief, National Security Division
MARK TAKLA (Cal. Bar No. 218111)
4 Assistant United States Attorney
Deputy Chief, Terrorism and Export Crimes Section
5 United States Attorney's Office
411 West Fourth Street, Suite 8000
6 Santa Ana, California 92701
Telephone: (714) 338-3591
7 Facsimile: (714) 338-3561
Email: mark.takla@usdoj.gov
8

Attorneys for Plaintiff
9 UNITED STATES OF AMERICA

10 UNITED STATES DISTRICT COURT

11 FOR THE CENTRAL DISTRICT OF CALIFORNIA

12 UNITED STATES OF AMERICA,

13 Plaintiff,

14 v.

15 JAMES ROBERT SCHWEITZER,

16 Defendant.
17
18

No. SA CR 20-188-JLS

GOVERNMENT'S SENTENCING POSITION;
EXHIBITS

Hearing Date: September 3, 2021

Hearing Time: 8:30 a.m.

19 Plaintiff United States of America, by and through its counsel
20 of record, the Acting United States Attorney for the Central District
21 of California and Assistant United States Attorney Mark Takla, hereby
22 files its Sentencing Position for defendant JAMES ROBERT SCHWEITZER.

23 //

24 //

25

26

27

28

1 This sentencing position is based upon the attached memorandum
2 of points and authorities, the Presentence Investigation Report, the
3 files and records in this case, and such further evidence and
4 argument as the Court may permit.

5 Dated: August 6, 2021

Respectfully submitted,

6 TRACY L. WILKISON
7 Acting United States Attorney

8 CHRISTOPHER D. GRIGG
9 Assistant United States Attorney
 Chief, National Security Division

10 /s/
11 MARK TAKLA
 Assistant United States Attorney

12 Attorneys for Plaintiff
13 UNITED STATES OF AMERICA
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MEMORANDUM OF POINTS AND AUTHORITIES

I. Introduction

Defendant James Robert Schweitzer - formerly a project engineer with a cleared Department of Defense ("DoD") contractor ("Company #1") - intentionally interfered with U.S. government communication lines by spamming unclassified DoD computer systems with classified national defense information causing cleanup costs of approximately \$15,000. Defendant pleaded guilty to one count of Malicious Interference with Communication Lines in violation of 18 U.S.C. § 1362.

The United States Probation Office ("USPO") filed its Presentence Investigation Report ("PSR"), concluding that: (1) defendant's base offense level is 6; (2) defendant's total offense level is 6 (applying a two-level enhancement for loss in excess of \$6,500 and applying a two-level reduction for acceptance of responsibility); (3) defendant's criminal history category is I; (4) defendant's guidelines sentencing range is 0 to 6 months of imprisonment; (5) defendant must pay a \$100 mandatory special assessment; and (6) defendant must pay restitution in the amount of \$15,000 and a fine in the amount of \$1,000. (PSR, at 3; Recommendation Letter, at 1-2.) The USPO recommended a sentence of two years of probation. (Id.)

The government agrees with the USPO's Guidelines calculation, recommended sentence, and recommended restitution order and fine. For the reasons outlined below, the government submits that this sentence is sufficient, but not greater than necessary, to achieve the goals of sentencing set forth in 18 U.S.C. § 3553(a).

1 **II. BACKGROUND**

2 The following facts are taken from the factual basis defendant
3 admitted to at his change of plea hearing:

4 Defendant JAMES ROBERT SCHWEITZER was formerly employed by
5 a defense contractor ("Company #1") located in the Central
6 District of California. Defendant worked as a software
7 engineer from 2003 through July 2016 and held a security
8 clearance from 2003/2004 until 2014. During his
employment, defendant worked on a Department of Defense
("DoD") program ("the DoD program"), portions of which were
classified. In 2014, defendant lost his security clearance
due to his use of medical marijuana.

9 In 2016, the defendant submitted a complaint to the DoD
10 Hotline, which is a website that can be used to make
11 whistleblower complaints. Defendant's complaint was later
12 determined to contain classified information. Also in 2015
13 or 2016, defendant began sending classified and national
14 defense information regarding the DoD program on
15 unclassified systems to DoD employees, Company #1
16 employees, and U.S. news outlets. In these communications,
defendant threatened to continue to disclose classified and
national defense information until he received a written
statement from DoD and Company #1 that DoD and Company #1
engaged in security violations defendant alleged to have
occurred. Defendant further stated that he intended to use
DoD's and Company #1's statements against them in a
lawsuit.

17 From April 2019 through March 2020, defendant emailed and
18 publicly posted classified and national defense information
19 related to the DoD program to a Social Media account he
20 operated (defendant's "Social Media Account"). Defendant
21 advertised his publication of classified and national
22 defense information on his Social Media Account via email
and other social media accounts he operated. Defendant
also emailed DoD employees, Company #1 employees, and U.S.
news outlets, advising them of his posting and inviting
them to visit his Social Media Account to view the
information.

23 At no time was defendant authorized to post or transmit
24 classified and national defense information. Defendant
25 knew that the public disclosure of such information was
26 likely to cause serious damage to national security and
27 that U.S. adversaries could take advantage of the
28 information defendant published online and transmitted to
persons without the required security clearances and using
unsecured systems.

From 2018 through May 2020, DoD and FBI personnel
repeatedly warned defendant against disclosing classified

1 and national defense information and transmitting
2 classified information on unclassified networks and using
3 unclassified communication facilities. Defendant ignored
4 these warnings and, in response to these warnings,
5 threatened to continue disclosing classified and national
6 defense information. For example, during a recorded May
7 21, 2020 telephone call with an FBI special agent,
8 defendant threatened to "contaminate . . . [at] least a dozen
9 government servers with classified data." On May 27, 2020,
10 defendant sent an email to several DoD employees with an
11 attachment containing classified and national defense
12 information and stated, "Be forewarned, each government and
13 [Company #1] recipient should lose at least a half day of
14 lost productivity (based on the process I was required to
15 follow as a cleared [Company #1] employee)."

16 As a result of defendant's unauthorized disclosures
17 including his May 27, 2020 email, DoD was forced to
18 undertake costly security protocols to purge classified and
19 national defense information from its unclassified computer
20 network and computer terminals. These safety procedures
21 interfered with DoD employees' ability to conduct their
22 duties, and DoD spent approximately \$15,000 to purge
23 classified and national defense information from DoD's
24 unclassified network and computer terminals.

25 Defendant admits that he willfully and maliciously injured
26 and interfered with the working of a communications systems
27 operated and controlled by the United States, namely, DoD's
28 unclassified network and computer terminals, by
transmitting classified and national defense information to
DoD's unclassified systems. At all times, defendant knew
that the communication systems would have to be purged of
the classified information, and intended to cause damage to
the communication systems by sending classified information
on them.

(Plea Agreement ¶ 10 (emphasis added).)

III. GUIDELINES CALCULATIONS

Consistent with the plea agreement, the USPO calculated a total
offense level of 6 based on the following calculation:

Base Offense Level:	6	U.S.S.G. § 2D1.1(a) (5)
Greater than \$6,500 in damage	+2	U.S.S.G. § 2D1.1(b) (12)
Acceptance of responsibility:	<u>-2</u>	U.S.S.G. § 3E1.1(a)-(b)
Total	6	

(PSR, at 3; Recommendation Letter, at 1-2.) Defendant is in criminal history category I. The government concurs with the USPO's guideline calculations and criminal history category. Defendant's guidelines range is 0 to 6 months of imprisonment.

IV. DEFENDANT'S OBJECTIONS TO THE PRESENTENCE REPORT

Paragraph 16. The government believes July 2016 is correct date when defendant began sending classified information. The government concurs that this is not a material dispute with the presentence report.

Paragraph 18. The government concurs that the call was on July 25, 2018.

Paragraphs 22 and 23. The government concurs the search was on November 14, 2018 and conducted by the U.S. Army Criminal Investigation Division.

The government does not object to the remaining of defendant's changes.

V. DEFENDANT'S MOTIVATION

Consistent with the plea agreement, the government continues to believe that a probationary sentence is appropriate. Nonetheless, a statement defendant made to the USPO warrants clarification. In his interview with the USPO, defendant appeared to claim an altruistic motive for committing the offense in this case. (PSR ¶ 35.)

("Schweitzer explained that a motivation he had for committing the instant offense, and his whistleblowing activities, was his worry adversarial countries of the United States would exploit, or had exploited, the vulnerabilities in his work."). Even if his interest in informing the DoD of security violations at his place of employment was altruistic and not the product of a personal workplace

1 grievance, his decision to expose national defense information by
2 posting it on public websites was a potentially dangerous act of
3 retaliation. This latter act was anything but altruistic. Moreover,
4 his statement to the USPO is inconsistent with both his actions and
5 his admissions to the FBI.

6 The government concurs that defendant initially made a DoD
7 Inspector General complaint. DoD found his first complaint - that he
8 was given incorrect advice about whether he could use medical
9 marijuana - substantiated. (Ex. A.) DoD found his second complaint
10 - that he inappropriately worked on a classified project without a
11 security clearance - unfounded. (Id.) Defendant was dissatisfied
12 with this response, therefore he knowingly began using classified
13 information to get DoD to pay attention to his complaints. (Ex. B.)
14 In the end, defendant used classified information and the threat of
15 dissemination of classified information in an attempt to obtain an
16 admission that his company and the DoD violated classified
17 information security protocols. (Ex. C (stating he hoped to get
18 "written apologies" and then stated "we need to talk about damages
19 and . . . penalties").) As defendant admitted in his factual basis,
20 defendant intended a lawsuit, (Plea Agreement ¶ 10; Ex. D), and
21 defendant needed an admission from the DoD regarding the security
22 violations at Company #1 in order to bring his lawsuit. Regardless
23 of whether DoD's determination of defendant's security violation
24 complaint was correct, defendant demonstrated a complete disregard
25 for the national security of the United States when he publicly
26 posted the classified national defense information online.

27 ///

Defendant posted the materials online knowing of the consequences of his action. As he admitted in his factual basis, "[d]efendant knew that the public disclosure of such information was likely to cause serious damage to national security and that U.S. adversaries could take advantage of the information defendant published online." (Plea Agreement ¶ 10.) Earlier, he told the FBI:

0
1 SM: Which, t-this, again, not meant to shock or reveal anything new, this is just confirming
2 stuff so we know, going forward, so we don't get too far off-track from each other. Umm ...
3 and that the information we've talked a little bit about what that information is with radar
4 and stuff, but that, the nature of that information is such that could result in uh, injury or
5 death of uh—
6
7 JS: [OV] Mhm—
8
9 SM: [OV] American equities, either abroad or locally. [background noise]
10
11 JS: Oh, yeah.
12
13 SM: [OV] Alright
14
15 JS: I totally, totally understand that, umm ... a-a-and I understand yeah, the-the ramifications
16 and the costs of that, as well, too ... yes—

(Ex. E.)¹

Defendant further stated:

19 JS: [OV] —because you guys have been listening, and you guys have been working with me,
20 as opposed to against me. You haven't intimidated or threatened me. You haven't
21 dismissed me. So no, we're working cooperatively together. Umm, my hope is that we
22 are going to find— and-and-and I-I know I cannot dictate schedule here. I get that, I get
23 that. Uh, but, as long as I see steady progress towards my truth, yeah. We're on the same
24 page. We're on the same page. It w- it was agonizing crossing that line to post this
25 stuff, because I am fully aware of the body count. [background noise] That's my phone,
26 which I'm going to ignore.

(Ex. F.)

¹ "JS" refers to defendant and "SM" are the initials of the interviewing FBI special agent.

1 Defendant posted classified national defense information on a
2 public website. His actions were not altruistic, but selfish.
3 Defendant made this information available to anyone who might come
4 across it, including adversaries of the United States with full
5 awareness of the "body count" or consequences of his actions. As a
6 result, the government's recommended sentence is consistent with the
7 plea agreement and strikes an appropriate balance among the statutory
8 sentencing factors.

9 **VI. CONCLUSION**

10 For the foregoing reasons, the government recommends the Court
11 sentence defendant to two years of probation, restitution in the
12 amount of \$15,000, a fine of \$1,000, and a mandatory special
13 assessment of \$100. The restitution payment is to be paid to the
14 following:

15 Defense Finance & Accounting Service
16 Department 3300
17 ATTN: Special Actions
8899 East 56th Street
Indianapolis, IN 46249-3300

DECLARATION OF MARK TAKLA

I, Mark Takla, declare as follows:

1. I am the Assistant United States Attorney assigned to this matter. I have knowledge of the facts set forth herein and could and would testify to those facts fully and truthfully if called and sworn as a witness.

2. Exhibit A is a true and correct copy of the Department of Defense response to defendant's Inspector General complaint from the investigative file.

3. Exhibit B is a true and correct copy of defendant's public social media posts from the investigative file.

4. Exhibits C through F are true and correct copies of a transcript of defendant's interviews with the FBI from the investigative file.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this declaration is executed in Santa Ana, California, on August 6, 2021.

Mark Takla

MARK TAKLA

DEFENDANTS' EXHIBIT 158:



HOME

ABOUT

DIVISIONS

NEWS

RESOURCES

COLLECTIONS

CONTACT



Online Alcohol Sales Concern Of Republican And Democrat Attorneys General

Landry-Frey Coalition Calls for Online Platforms to Crack Down on Illegal Sales

BATON ROUGE, LA – A bipartisan coalition of 46 state and territory Attorneys General – led by Louisiana Attorney General Jeff Landry and Maine Attorney General Aaron Frey – called on Facebook, Craigslist, and eBay to take proactive measures against alcohol sales on their platforms which frequently violate state laws and could pose health risks.

“As we have seen recently with vaping and opioids, adolescents are finding new ways to purchase contraband online,” said Attorney General Landry. “These widely-used online platforms have a responsibility to implement meaningful systems and programs that proactively address this problem and keep our children safe.”

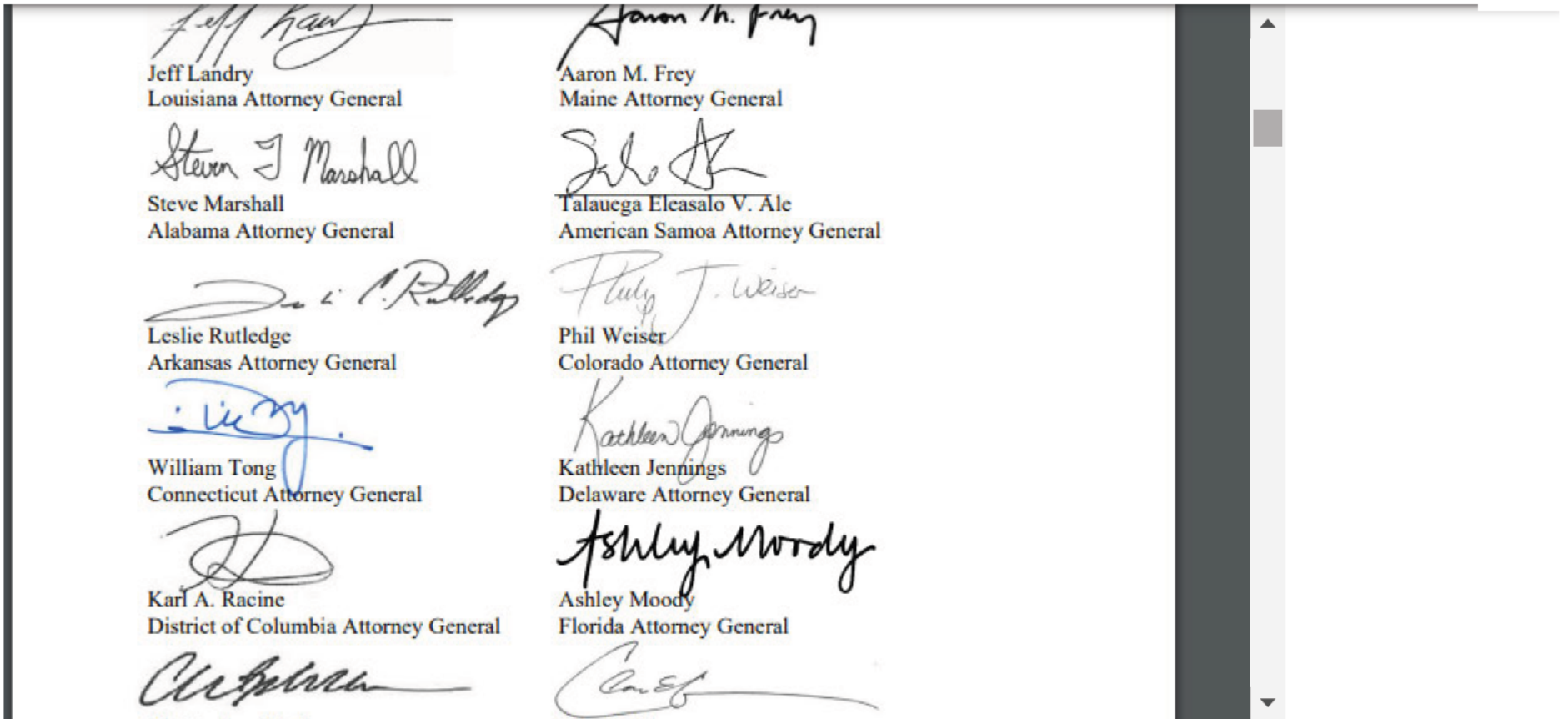
In letters to the online platforms, the Attorneys General argue that “everyone has an ethical and moral responsibility to protect consumers, especially those who are most vulnerable to fraud.” They note that the 21st Amendment invests the right to regulate the sale of alcohol to each state and point out concerns that unlicensed, unregulated, and untaxed alcohol sales are taking place on digital platforms.

“The black-market products sold on these platforms may be counterfeit or tainted, sometimes with harmful health effects,” warned General Landry. “So together – Republican and Democrat – we want to solve this problem and make our jurisdictions safer places to live, work, and raise families.”

The Attorneys General ask Facebook, Craigslist, and eBay to review the current content posted to the companies’ websites and remove any illegal postings for the sales and/or transfer of alcohol products. They also ask the platforms to work to develop and deploy programming to block and prevent their platform users from violating state law by posting content for the sale and distribution of alcohol products on their websites.

Joining General Landry and General Frey in signing the letters are the Attorneys General of Alabama, American Samoa, Arkansas, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Puerto Rico, Rhode Island, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Washington, West Virginia, and Wisconsin.

[NAAGLettersCombined-OnlineSaleofAlcohol.pdf](#)



Search



Latest News

Major Victory for New Orleans: Consent Decree Overreach Blocked by Appeals Court

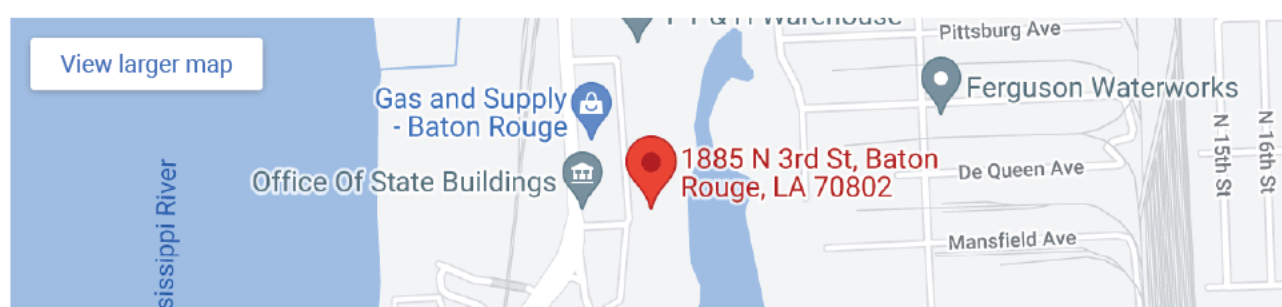
4/12/2023

New Orleans Consent Decree Threatens Proper Balance Between State and Federal Powers Argues Attorney General Jeff Landry

4/11/2023

Biden's Latest Attack on Gas Stoves Met with Opposition by Louisiana-led Coalition of Attorneys General

4/3/2023



Newsletter

Sign Up

Be the first to find out about the latest legal news, updates, tips, and other information.

© 2023 Louisiana Department of Justice.



DEFENDANTS' EXHIBIT 159:



PRESIDENT
Jeff Landry

Louisiana Attorney General

PRESIDENT-ELECT
Tim Fox

Montana Attorney General

VICE PRESIDENT
Karl A. Racine
*District of Columbia
Attorney General*

IMMEDIATE PAST PRESIDENT
Derek Schmidt
Kansas Attorney General

EXECUTIVE DIRECTOR
Chris Toth

October 22, 2019

Scott Schenkel
eBay Interim Chief Executive Officer
2025 Hamilton Avenue
San Jose, California 95125

Mr. Schenkel:

Social media and digital platforms have become interwoven into the fabric of our society. Consumers have become increasingly dependent on the broad access to goods for sale through these mediums. Unfortunately, the near-unlimited access to goods has increasingly exposed consumers, including minors, to unlicensed sales of alcohol and counterfeit products. We are seeking your assistance to address some of the challenges to consumer protection associated with online marketplaces and to improve the legitimacy of these sales.

We are aware of the occurrence of unlicensed, unregulated, and untaxed alcohol sales through digital platforms. Some of the products sold in this manner may be counterfeit, mislabeled, or fraudulent. The consumer may not know that this method of alcohol sales is illegitimate, or that these black-market products could pose health risks. Bad actors may exploit the anonymity of a digital platform to evade regulation, law enforcement, taxation and responsibility.

The 21st Amendment to the U.S. Constitution firmly invests the right to regulate the sale of alcoholic beverages with each state. Each online content company operating within the United States has a legal obligation to comply with federal and state law. But that is simply a legal obligation. We believe that everyone has an ethical and moral responsibility to protect consumers, especially those who are most vulnerable to fraud. Self-regulation and self-policing to prevent illegal and unfair trade practices and ensure consumer safety are minimum responsibilities for your respective companies. You have the technical prowess and power to accomplish basic protections against illegal sales.

Today, we call upon you to join us in this shared responsibility to protect our youth, the Constitution and the integrity of the digital marketplace. Toward this goal, we ask your companies to undertake some initial steps to address this shared problem:

1. Review the current content posted to your companies' websites and remove illegal postings for the sales and/or transfer of alcohol products.

1850 M Street, NW
Twelfth Floor
Washington, DC 20036
Phone: (202) 326-6000
<http://www.naag.org/>

2. Develop and deploy programming to block and prevent your platform users from violating state law by posting content for the sale and distribution of alcohol products on your websites.

We also invite you to join with us to establish a workgroup with stakeholders from industry and government. Together, this group can discuss and establish realistic and effective protocols for internet platforms and content providers related to illegal and unlicensed alcohol sales via digital platforms.

Thank you for your prompt attention to this matter. We would appreciate hearing from you about the actions your company has taken, or will take, to protect consumers in the online marketplace. We know that by working together we can harness the great power of your platform and the great responsibility invested in our offices to address these harmful and illegal activities.

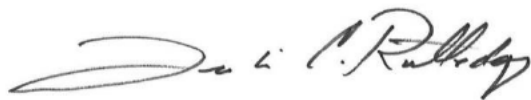
Sincerely,



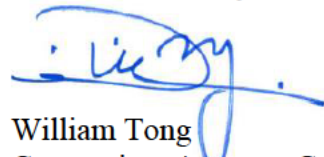
Jeff Landry
Louisiana Attorney General



Steve Marshall
Alabama Attorney General



Leslie Rutledge
Arkansas Attorney General



William Tong
Connecticut Attorney General



Karl A. Racine
District of Columbia Attorney General



Christopher M. Carr
Georgia Attorney General



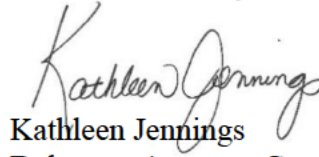
Aaron M. Frey
Maine Attorney General



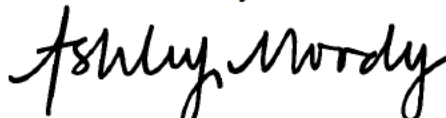
Talauega Eleasalo V. Ale
American Samoa Attorney General



Phil Weiser
Colorado Attorney General



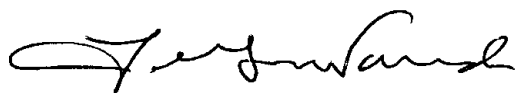
Kathleen Jennings
Delaware Attorney General



Ashley Moody
Florida Attorney General



Clare E. Connors
Hawaii Attorney General



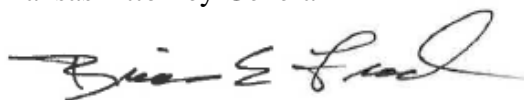
Lawrence Wasden
Idaho Attorney General



Curtis T. Hill, Jr.
Indiana Attorney General



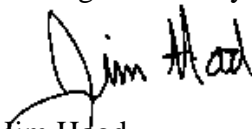
Derek Schmidt
Kansas Attorney General



Brian Frosh
Maryland Attorney General



Dana Nessel
Michigan Attorney General



Jim Hood
Mississippi Attorney General



Douglas Peterson
Nebraska Attorney General



Gurbir S. Grewal
New Jersey Attorney General



Letitia James
New York Attorney General



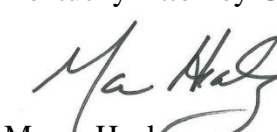
Kwame Raoul
Illinois Attorney General



Tom Miller
Iowa Attorney General



Andy Beshear
Kentucky Attorney General



Maura Healey
Massachusetts Attorney General



Keith Ellison
Minnesota Attorney General



Tim Fox
Montana Attorney General



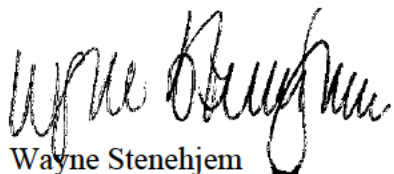
Aaron D. Ford
Nevada Attorney General



Hector Balderas
New Mexico Attorney General



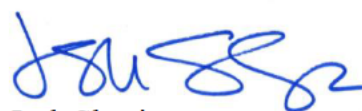
Josh Stein
North Carolina Attorney General



Wayne Stenehjem
North Dakota Attorney General



Mike Hunter
Oklahoma Attorney General



Josh Shapiro
Pennsylvania Attorney General



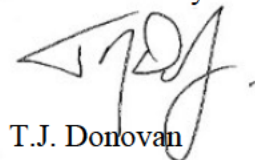
Peter F. Neronha
Rhode Island Attorney General



Jason R. Ravensborg
South Dakota Attorney General



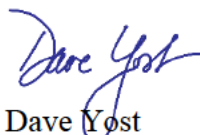
Ken Paxton
Texas Attorney General



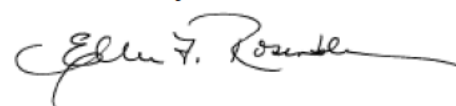
T.J. Donovan
Vermont Attorney General



Patrick Morrissey
West Virginia Attorney General



Dave Yost
Ohio Attorney General



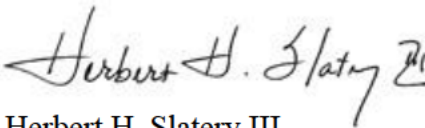
Ellen F. Rosenblum
Oregon Attorney General



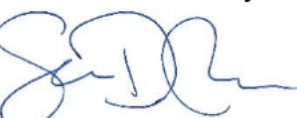
Dennise N. Longo Quiñones
Puerto Rico Attorney General



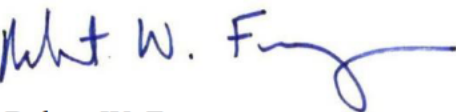
Alan Wilson
South Carolina Attorney General



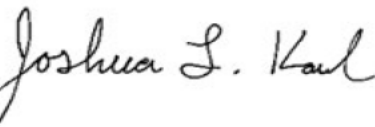
Herbert H. Slatery III
Tennessee Attorney General



Sean Reyes
Utah Attorney General



Robert W. Ferguson
Washington Attorney General



Joshua L. Kaul
Wisconsin Attorney General



PRESIDENT
Jeff Landry

Louisiana Attorney General

PRESIDENT-ELECT
Tim Fox

Montana Attorney General

VICE PRESIDENT
Karl A. Racine
*District of Columbia
Attorney General*

IMMEDIATE PAST PRESIDENT
Derek Schmidt
Kansas Attorney General

EXECUTIVE DIRECTOR
Chris Toth

October 22, 2019

Mark Zuckerberg
Facebook Chief Executive Officer
1 Hacker Way
Menlo Park, CA 94025

Mr. Zuckerberg:

Social media and digital platforms have become interwoven into the fabric of our society. Consumers have become increasingly dependent on the broad access to goods for sale through these mediums. Unfortunately, the near-unlimited access to goods has increasingly exposed consumers, including minors, to unlicensed sales of alcohol and counterfeit products. We are seeking your assistance to address some of the challenges to consumer protection associated with online marketplaces and to improve the legitimacy of these sales.

We are aware of the occurrence of unlicensed, unregulated, and untaxed alcohol sales through digital platforms. Some of the products sold in this manner may be counterfeit, mislabeled, or fraudulent. The consumer may not know that this method of alcohol sales is illegitimate, or that these black-market products could pose health risks. Bad actors may exploit the anonymity of a digital platform to evade regulation, law enforcement, taxation and responsibility.

The 21st Amendment to the U.S. Constitution firmly invests the right to regulate the sale of alcoholic beverages with each state. Each online content company operating within the United States has a legal obligation to comply with federal and state law. But that is simply a legal obligation. We believe that everyone has an ethical and moral responsibility to protect consumers, especially those who are most vulnerable to fraud. Self-regulation and self-policing to prevent illegal and unfair trade practices and ensure consumer safety are minimum responsibilities for your respective companies. You have the technical prowess and power to accomplish basic protections against illegal sales.

Today, we call upon you to join us in this shared responsibility to protect our youth, the Constitution and the integrity of the digital marketplace. Toward this goal, we ask your companies to undertake some initial steps to address this shared problem:

1. Review the current content posted to your companies' websites and remove illegal postings for the sales and/or transfer of alcohol products.

1850 M Street, NW
Twelfth Floor
Washington, DC 20036
Phone: (202) 326-6000
<http://www.naag.org/>

2. Develop and deploy programming to block and prevent your platform users from violating state law by posting content for the sale and distribution of alcohol products on your websites.

We also invite you to join with us to establish a workgroup with stakeholders from industry and government. Together, this group can discuss and establish realistic and effective protocols for internet platforms and content providers related to illegal and unlicensed alcohol sales via digital platforms.

Thank you for your prompt attention to this matter. We would appreciate hearing from you about the actions your company has taken, or will take, to protect consumers in the online marketplace. We know that by working together we can harness the great power of your platform and the great responsibility invested in our offices to address these harmful and illegal activities.

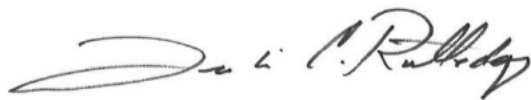
Sincerely,



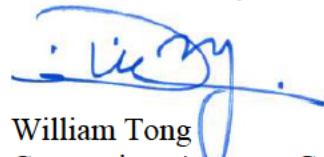
Jeff Landry
Louisiana Attorney General



Steve Marshall
Alabama Attorney General



Leslie Rutledge
Arkansas Attorney General



William Tong
Connecticut Attorney General



Karl A. Racine
District of Columbia Attorney General



Christopher M. Carr
Georgia Attorney General



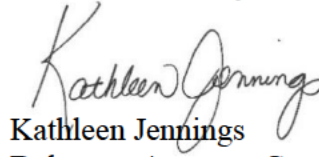
Aaron M. Frey
Maine Attorney General



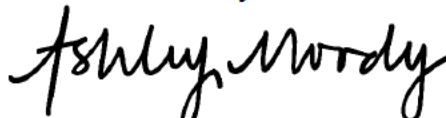
Talauega Eleasalo V. Ale
American Samoa Attorney General



Phil Weiser
Colorado Attorney General



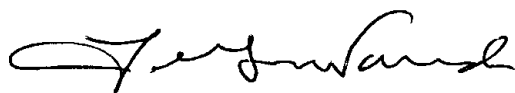
Kathleen Jennings
Delaware Attorney General



Ashley Moody
Florida Attorney General



Clare E. Connors
Hawaii Attorney General



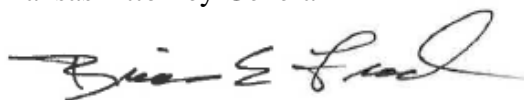
Lawrence Wasden
Idaho Attorney General



Curtis T. Hill, Jr.
Indiana Attorney General



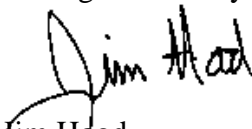
Derek Schmidt
Kansas Attorney General



Brian Frosh
Maryland Attorney General



Dana Nessel
Michigan Attorney General



Jim Hood
Mississippi Attorney General




Douglas Peterson
Nebraska Attorney General



Gurbir S. Grewal
New Jersey Attorney General



Letitia James
New York Attorney General



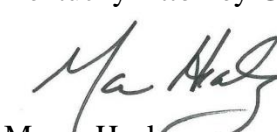
Kwame Raoul
Illinois Attorney General



Tom Miller
Iowa Attorney General



Andy Beshear
Kentucky Attorney General



Maura Healey
Massachusetts Attorney General



Keith Ellison
Minnesota Attorney General



Tim Fox
Montana Attorney General



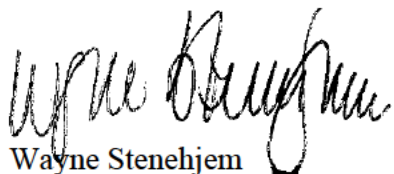
Aaron D. Ford
Nevada Attorney General



Hector Balderas
New Mexico Attorney General



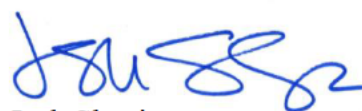
Josh Stein
North Carolina Attorney General



Wayne Stenehjem
North Dakota Attorney General



Mike Hunter
Oklahoma Attorney General



Josh Shapiro
Pennsylvania Attorney General



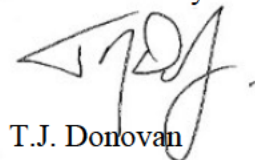
Peter F. Neronha
Rhode Island Attorney General



Jason R. Ravensborg
South Dakota Attorney General



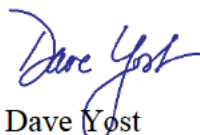
Ken Paxton
Texas Attorney General



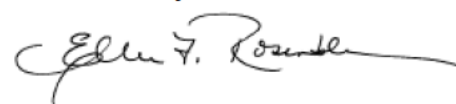
T.J. Donovan
Vermont Attorney General



Patrick Morrissey
West Virginia Attorney General



Dave Yost
Ohio Attorney General



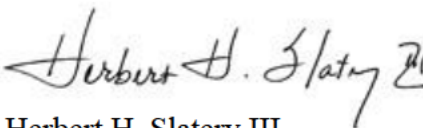
Ellen F. Rosenblum
Oregon Attorney General



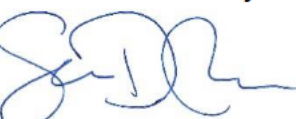
Dennise N. Longo Quiñones
Puerto Rico Attorney General



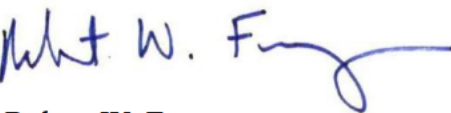
Alan Wilson
South Carolina Attorney General



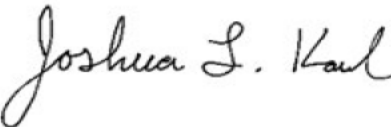
Herbert H. Slatery III
Tennessee Attorney General



Sean Reyes
Utah Attorney General



Robert W. Ferguson
Washington Attorney General



Joshua L. Kaul
Wisconsin Attorney General



PRESIDENT
Jeff Landry

Louisiana Attorney General

PRESIDENT-ELECT
Tim Fox

Montana Attorney General

VICE PRESIDENT
Karl A. Racine
*District of Columbia
Attorney General*

IMMEDIATE PAST PRESIDENT
Derek Schmidt
Kansas Attorney General

EXECUTIVE DIRECTOR
Chris Toth

October 22, 2019

Jim Buckmaster
Craigslist Chief Executive Officer
1381 9th Ave.
San Francisco, CA 94122

Mr. Buckmaster:

Social media and digital platforms have become interwoven into the fabric of our society. Consumers have become increasingly dependent on the broad access to goods for sale through these mediums. Unfortunately, the near-unlimited access to goods has increasingly exposed consumers, including minors, to unlicensed sales of alcohol and counterfeit products. We are seeking your assistance to address some of the challenges to consumer protection associated with online marketplaces and to improve the legitimacy of these sales.

We are aware of the occurrence of unlicensed, unregulated, and untaxed alcohol sales through digital platforms. Some of the products sold in this manner may be counterfeit, mislabeled, or fraudulent. The consumer may not know that this method of alcohol sales is illegitimate, or that these black-market products could pose health risks. Bad actors may exploit the anonymity of a digital platform to evade regulation, law enforcement, taxation and responsibility.

The 21st Amendment to the U.S. Constitution firmly invests the right to regulate the sale of alcoholic beverages with each state. Each online content company operating within the United States has a legal obligation to comply with federal and state law. But that is simply a legal obligation. We believe that everyone has an ethical and moral responsibility to protect consumers, especially those who are most vulnerable to fraud. Self-regulation and self-policing to prevent illegal and unfair trade practices and ensure consumer safety are minimum responsibilities for your respective companies. You have the technical prowess and power to accomplish basic protections against illegal sales.

Today, we call upon you to join us in this shared responsibility to protect our youth, the Constitution and the integrity of the digital marketplace. Toward this goal, we ask your companies to undertake some initial steps to address this shared problem:

1. Review the current content posted to your companies' websites and remove illegal postings for the sales and/or transfer of alcohol products.

1850 M Street, NW
Twelfth Floor
Washington, DC 20036
Phone: (202) 326-6000
<http://www.naag.org/>

2. Develop and deploy programming to block and prevent your platform users from violating state law by posting content for the sale and distribution of alcohol products on your websites.

We also invite you to join with us to establish a workgroup with stakeholders from industry and government. Together, this group can discuss and establish realistic and effective protocols for internet platforms and content providers related to illegal and unlicensed alcohol sales via digital platforms.

Thank you for your prompt attention to this matter. We would appreciate hearing from you about the actions your company has taken, or will take, to protect consumers in the online marketplace. We know that by working together we can harness the great power of your platform and the great responsibility invested in our offices to address these harmful and illegal activities.

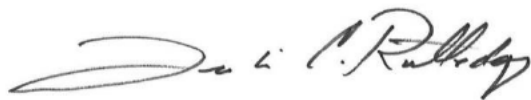
Sincerely,



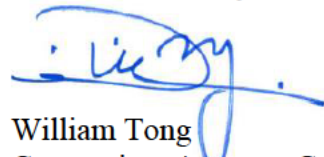
Jeff Landry
Louisiana Attorney General



Steve Marshall
Alabama Attorney General



Leslie Rutledge
Arkansas Attorney General



William Tong
Connecticut Attorney General



Karl A. Racine
District of Columbia Attorney General



Christopher M. Carr
Georgia Attorney General



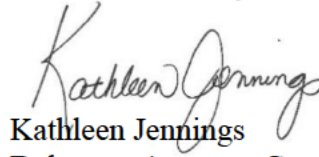
Aaron M. Frey
Maine Attorney General



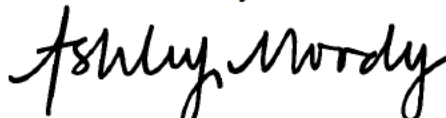
Talauega Eleasalo V. Ale
American Samoa Attorney General



Phil Weiser
Colorado Attorney General



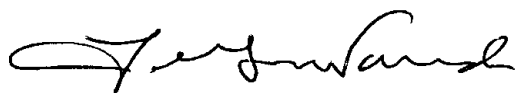
Kathleen Jennings
Delaware Attorney General



Ashley Moody
Florida Attorney General



Clare E. Connors
Hawaii Attorney General



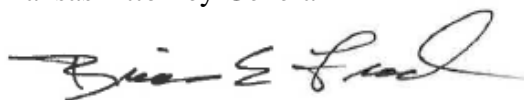
Lawrence Wasden
Idaho Attorney General



Curtis T. Hill, Jr.
Indiana Attorney General



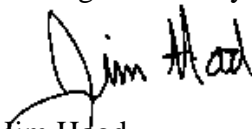
Derek Schmidt
Kansas Attorney General



Brian Frosh
Maryland Attorney General



Dana Nessel
Michigan Attorney General



Jim Hood
Mississippi Attorney General



Douglas Peterson
Nebraska Attorney General



Gurbir S. Grewal
New Jersey Attorney General



Letitia James
New York Attorney General



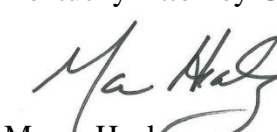
Kwame Raoul
Illinois Attorney General



Tom Miller
Iowa Attorney General



Andy Beshear
Kentucky Attorney General



Maura Healey
Massachusetts Attorney General



Keith Ellison
Minnesota Attorney General



Tim Fox
Montana Attorney General



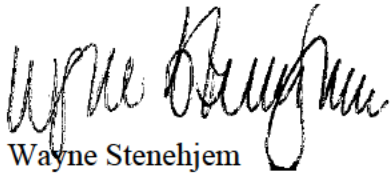
Aaron D. Ford
Nevada Attorney General



Hector Balderas
New Mexico Attorney General



Josh Stein
North Carolina Attorney General



Wayne Stenehjem
North Dakota Attorney General



Mike Hunter
Oklahoma Attorney General



Josh Shapiro
Pennsylvania Attorney General



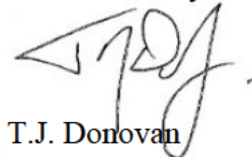
Peter F. Neronha
Rhode Island Attorney General



Jason R. Ravensborg
South Dakota Attorney General



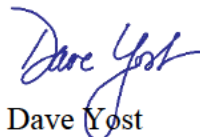
Ken Paxton
Texas Attorney General



T.J. Donovan
Vermont Attorney General



Patrick Morrissey
West Virginia Attorney General



Dave Yost
Ohio Attorney General



Ellen F. Rosenblum
Oregon Attorney General



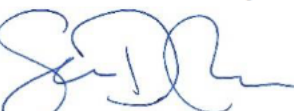
Dennise N. Longo Quiñones
Puerto Rico Attorney General



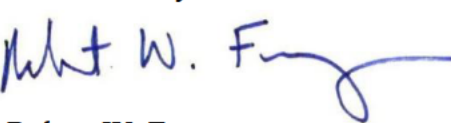
Alan Wilson
South Carolina Attorney General



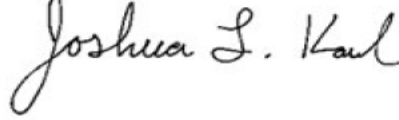
Herbert H. Slatery III
Tennessee Attorney General



Sean Reyes
Utah Attorney General



Robert W. Ferguson
Washington Attorney General



Joshua L. Kaul
Wisconsin Attorney General

DEFENDANTS' EXHIBIT 160:



33 State Attorneys General Warn Amazon, Facebook, Ebay, Craigslist, Walmart: Online Marketplaces Are Not Exempt From Price Gouging Laws

BATON ROUGE, LA – Louisiana Attorney General Jeff Landry has joined with 32 of his fellow state attorneys general in urging Amazon, Facebook, Ebay, Walmart, and Craigslist to more rigorously monitor price gouging practices by online sellers using their services.

“We want the business community and American consumers to know that we endeavor to balance the twin imperatives of commerce and consumer protection in the marketplace,” said General Landry and his colleagues in letters to the retail giants. “And, while we appreciate reports of the efforts made by platforms and online retailers to crack down on price gouging as the American community faces an unprecedented public health crisis, we are calling on you to do more at a time that requires national unity.”

The letters list several examples of price-gouging on these marketplace platforms, all of which took place only in March: on Craigslist, a two-liter bottle of hand sanitizer was being sold for \$250; on Facebook Marketplace, an eight-ounce bottle was being sold for \$40; and on Ebay, packs of face masks were being sold for \$40 and \$50.

General Landry and the attorney general coalition recommended changes to protect consumers from price gouging:

Set policies and enforce restrictions on unconscionable price gouging during emergencies: Online retail platforms should prevent unconscionable price increases from occurring by creating and enforcing strong policies that prevent sellers from deviating in any significant way from the product’s price before an emergency. Such policies should examine historical seller prices, and the price offered by other sellers of the same or similar products, to identify and eliminate price gouging.

Trigger price gouging protections prior to an emergency declaration, such as when your systems detect conditions like pending weather events or future possible health risks.

Implement a complaint portal for consumers to report potential price gouging.

General Landry continues to encourage consumers to report suspected price gouging to their local law enforcement as, in certain situations, price gouging is a crime. Additionally, he asks that consumer disputes be filed with his office as they may be able to seek a civil penalty and civil restitution against an offender. In both, General Landry encourages consumers to provide specific evidence supporting the complaint, including advertisements and receipts of the product or service.

Joining the Louisiana AG on this effort were the attorneys general from Connecticut, New Mexico, Pennsylvania, Vermont, California, Colorado, Delaware, District of Columbia, Hawaii, Idaho, Illinois, Iowa, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oregon, Rhode Island, Utah, Virginia, Washington, Wyoming, and Puerto Rico.

#

Copies of the letters may be found below.

[eBay.pdf](#) [view](#)

[Facebook.pdf](#) [view](#)

[Craigslist.pdf](#) [view](#)

[Walmart.pdf](#) [view](#)

[Amazon.pdf](#) [view](#)

Search



Latest News

Major Victory for New Orleans: Consent Decree Overreach Blocked by Appeals Court

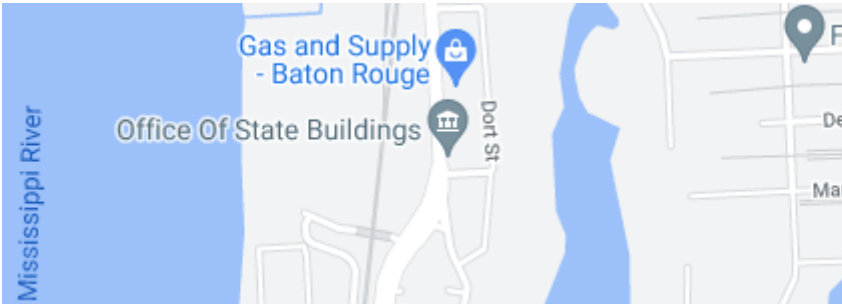
4/12/2023

New Orleans Consent Decree Threatens Proper Balance Between State and Federal Powers Argues Attorney General Jeff Landry

4/11/2023

Biden’s Latest Attack on Gas Stoves Met with Opposition by Louisiana-led Coalition of Attorneys General

4/3/2023



Newsletter

Sign Up

Be the first to find out about the latest legal news,
updates, tips, and other information.

DEFENDANTS' EXHIBIT 161:



NATIONAL
ASSOCIATION OF
ATTORNEYS GENERAL

PRESIDENT

District of Columbia
Attorney General

PRESIDENT-ELECT

Iowa
Attorney General

VICE PRESIDENT

North Carolina
Attorney General

IMMEDIATE PAST
PRESIDENT

Louisiana
Attorney General

Executive Director

April 1, 2021

Via First Class and Electronic Mail

Jack Dorsey
Chief Executive Officer
Twitter, Inc.
1355 Market St. San Francisco, CA 94103

Tobias Lütke
Chief Executive Officer
Shopify
33 New Montgomery St #750
San Francisco, CA 94105

Jamie Iannone
Chief Executive Officer
eBay, Inc.
2025 Hamilton Avenue
San Jose, California 95125

Re: Deceptive marketing and sales of fake COVID vaccine cards

Dear Messrs. Dorsey, Lütke and Iannone

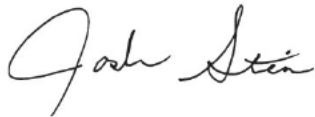
The undersigned attorneys general are committed to protecting the safety and well-being of the residents of our states. It has come to our attention that your platforms are being used to market and sell blank or fraudulently completed COVID vaccine cards bearing the Centers for Disease Control and Prevention logo.

We are deeply concerned about this use of your platforms to spread false and misleading information regarding COVID vaccines. The false and deceptive marketing and sales of fake COVID vaccine cards threatens the health of our communities, slows progress in getting our residents protected from the virus, and are a violation of the laws of many states. Multiple states' laws provide for injunctive relief, damages, penalties, and other remedies for such conduct.

The use of your platforms to disseminate the deceptive marketing and sales of fake vaccine cards is a threat to residents of our states. As a result, we are asking you to take immediate action to prevent your platforms from being used as a vehicle to commit these fraudulent and deceptive acts that harm our communities. Such action should include, without limitation: (1) monitoring your platforms for ads or links marketing or selling, or otherwise indicating the availability of, blank or fraudulently completed vaccine cards; (2) promptly taking down ads or links identified through that monitoring; and (3) preserving records, such as the content, username, and actual user identity, pertaining to any such ads or links.

We would appreciate a response to this request by April 9, 2021 setting forth how you intend to comply with the foregoing. We are also available for a virtual meeting to further discuss our concerns. We look forward to your timely response.

Sincerely,



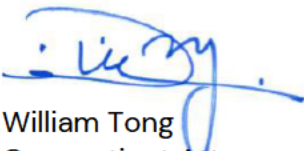
Josh Stein
North Carolina Attorney General



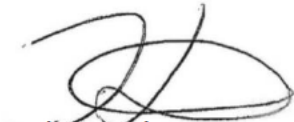
Treg R. Taylor
Alaska Attorney General



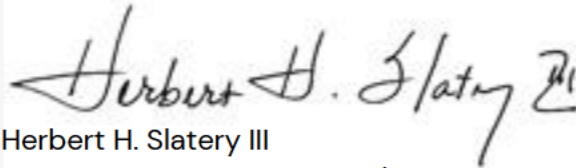
Matthew Rodriguez
Acting California Attorney General



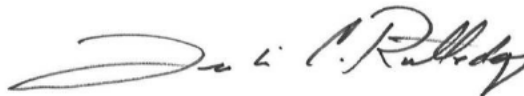
William Tong
Connecticut Attorney General



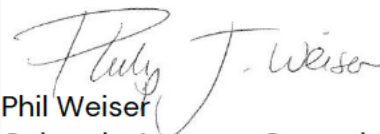
Karl A. Racine
District of Columbia Attorney General



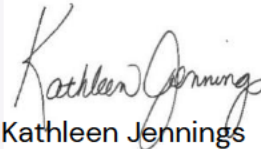
Herbert H. Slatery III
Tennessee Attorney General



Leslie Rutledge
Arkansas Attorney General



Phil Weiser
Colorado Attorney General



Kathleen Jennings
Delaware Attorney General



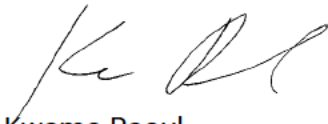
Ashley Moody
Florida Attorney General



Christopher M. Carr
Georgia Attorney General



Leevin Taitano Camacho
Guam Attorney General



Kwame Raoul
Illinois Attorney General



Tom Miller
Iowa Attorney General



Derek Schmidt
Kansas Attorney General



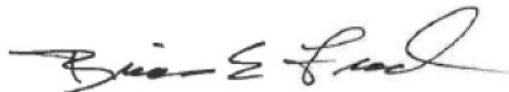
Daniel Cameron
Kentucky Attorney General



Jeff Landry
Louisiana Attorney General



Aaron M. Frey
Maine Attorney General



Brian Frosh
Maryland Attorney General



Maura Healey
Massachusetts Attorney General



Dana Nessel
Michigan Attorney General



Keith Ellison
Minnesota Attorney General



Douglas Peterson
Nebraska Attorney General



Aaron D. Ford
Nevada Attorney General



Jane E. Young
New Hampshire Deputy Attorney General



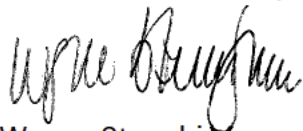
Gurbir S. Grewal
New Jersey Attorney General



Hector Balderas
New Mexico Attorney General



Letitia James
New York Attorney General



Wayne Stenehjem
North Dakota Attorney General




Edward Manibusan
Northern Mariana Islands Attorney General



Dave Yost
Ohio Attorney General



Mike Hunter
Oklahoma Attorney General



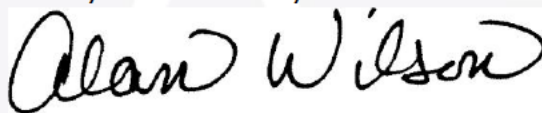
Ellen F. Rosenblum
Oregon Attorney General



Josh Shapiro
Pennsylvania Attorney General



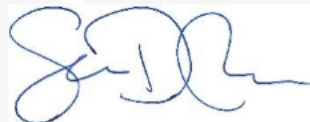
Peter F. Neronha
Rhode Island Attorney General



Alan Wilson
South Carolina Attorney General



Jason R. Ravensborg
South Dakota Attorney General



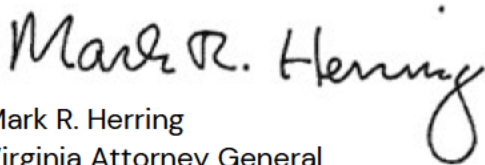
Sean Reyes
Utah Attorney General



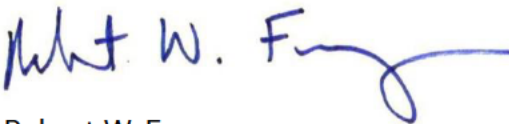
Denise N. George
U.S. Virgin Islands Attorney General



T.J. Donovan
Vermont Attorney General



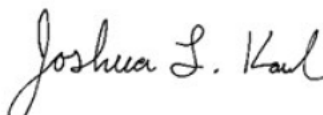
Mark R. Herring
Virginia Attorney General



Robert W. Ferguson
Washington Attorney General



Patrick Morrissey
West Virginia Attorney General



Joshua L. Kaul
Wisconsin Attorney General

Bridget Hill

Bridget Hill
Wyoming Attorney General



DEFENDANTS' EXHIBIT 162:

Benadryl TikTok 'challenge': A 13-year-old died in Ohio after participating

 [cnn.com/2023/04/18/u/benadryl-tiktok-challenge-teen-death-wellne/index.html](https://www.cnn.com/2023/04/18/u/benadryl-tiktok-challenge-teen-death-wellne/index.html)

Michelle Watson, Carma Hassan

April 18, 2023



Jacob was on a ventilator for almost a week before he died, according to CNN affiliate WSYX.

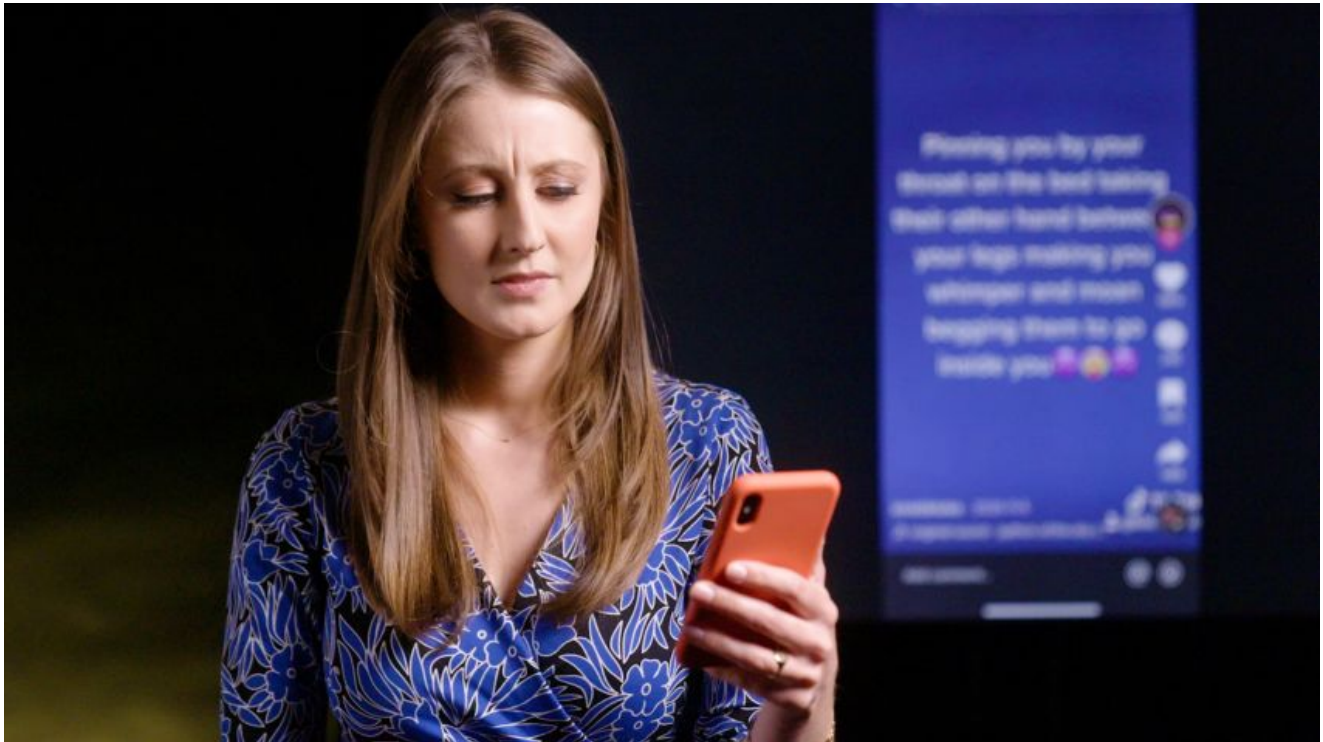
From GoFundMe/Jacob Stevens
CNN —

A 13-year-old in Ohio has died after “he took a bunch of Benadryl,” trying a dangerous TikTok challenge that’s circulating online, according to a CNN affiliate and a GoFundMe account from his family.

Jacob Stevens was participating in a TikTok challenge with some friends at home when he ingested the antihistamine, the family donation account states. Jacob was on a ventilator for almost a week before he died, according to WSYX.

CNN has not independently confirmed his cause of death

Overdosing on Benadryl can result in “serious heart problems, seizures, coma, or even death,” the US Food and Drug Administration said in a 2020 warning to the public about the deadly “Benadryl Challenge” on TikTok.



CNN takes over a 14 year old's TikTok account 17 minutes in, this is what we saw

06:47 - Source: CNN Business

Jacob's grandmother is doing anything she can "to make sure another child doesn't go through" with the challenge, she told CNN affiliate WSYX

In a statement to CNN, TikTok said, "Our deepest sympathies go out to the family. At TikTok, we strictly prohibit and remove content that promotes dangerous behavior with the safety of our community as a priority. We have never seen this type of content trend on our platform and have blocked searches for years to help discourage copycat behavior. Our team of 40,000 safety professionals works to remove violations of our Community Guidelines and we encourage our community to report any content or accounts they're concerned about."



The allergy drug Claritin sits on a shelf next to Benadryl in a pharmacy December 11, 2002 in New York City. The drug is now available in stores nationwide without a prescription. (Photo by Mario Tama/Getty Images)

Mario Tama/Getty Images

FDA issues Benadryl warning as it investigates reports of teen injuries and deaths linked to TikTok challenge

The maker of Benadryl, Johnson & Johnson, has called the challenge “dangerous.”

“We understand that consumers may have heard about an online ‘challenge’ involving the misuse or abuse of diphenhydramine,” the undated online statement reads

“The challenge, which involves ingestion of excessive quantities of diphenhydramine, is a dangerous trend and should be stopped immediately BENADRYL® products and other diphenhydramine products should only be used as directed by the label.”

“We are working with TikTok and other social platforms to remove content that showcases this behavior,” the statement added “We will look to partner across industry and with key stakeholders to address this dangerous behavior.”

CNN has reached out to the Stevens family and Columbus Public Health for comment

The FDA's 2020 warning said the agency had “contacted TikTok and strongly urged them to remove the videos from their platform and to be vigilant to remove additional videos that may be posted ”

Benadryl is an antihistamine used to treat symptoms such as a runny nose or sneezing from upper respiratory allergies, hay fever or the common cold. It's safe and effective when used as recommended, the FDA said.

"Diphenhydramine is marketed under the brand-name Benadryl, store brands, and generics. It is also available in combination with pain relievers, fever reducers, and decongestants," the agency said.

Consumers and parents should store Benadryl and other over the counter medications and prescription medicines out of the reach of children, the FDA said.

CNN's Jamie Gumbrecht and Travis Nichols contributed to this report.

DEFENDANTS' EXHIBIT 163:

2016 WL 3523926

Roll Call, Inc.

Copyright (c) 2016 CQ-Roll Call, Inc.

Testimony

June 28, 2016

Senate

Foreign Relations

Global Efforts to Defeat Isis

Statement of Brett H. McGurk
Special Presidential Envoy
Global Coalition to Counter ISIL

Committee on Senate Foreign Relations

June 28, 2016

Introduction

Chairman Corker, Ranking Member Cardin, esteemed members of the committee, thank you for providing me the opportunity to update you on our global campaign to defeat ISIL.

The fight against ISIL is an unprecedented challenge. More than 40,000 foreign fighters have flowed into Syria over the past five years, swelling the ranks of violent extremist organizations, the most significant of which is ISIL. ISIL is determined to establish a state in Iraq and Syria, and instill terror around the world as part of a perverse agenda, whereby, according to their own ideology, anyone who disagrees with them should die. We have no choice but to defeat ISIL by taking away its territory in Iraq and Syria, severing its global networks, and suffocating its global affiliates.

I will describe today the progress we are making in all of these areas, but this progress does not discount the significant threat that remains, and will remain, for years to come. As an entire government, and as a country, we must remain vigilant, committed to a sustainable, global, and long-term effort to defeat ISIL, and ensure that other violent extremist groups, such as Jabhat al Nusra, al Qaida's official affiliate in Syria, cannot rise from its ashes. The support of this Committee and the Congress will be essential to our success, and it is my honor to appear before you again for an update on our campaign.

Diagnosing the ISIL Threat

We analyze the ISIL challenge in three dimensions: the core in Iraq and Syria (its phony selfproclaimed 'caliphate'); the global networks (foreign fighter, financial, and messaging networks); and the global affiliates (eight in all, with some far more serious than others). Any successful campaign must address all three, and our global effort, anchored by a coalition of 66 partners, is designed to do just that.

At the same time, the ISIL core remains its center of gravity, allowing ISIL to extract resources, recruit, and plan sophisticated external terrorist attacks, as we have seen in Paris and Brussels. Thus, we are focused first and foremost on shrinking the core, uprooting ISIL from the cities, towns, and villages under its control, and destroying its underlying infrastructure, including the human capital of its leaders, now being eliminated one-by-one.

Current Assessment

In July 2014, I testified before this committee as ISIL was expanding its territory, threatening Baghdad, and appeared unstoppable. The situation today is measurably different. ISIL has not launched a significant offensive in over a year; it is losing cities - Tikrit, Ramadi, Fallujah, Hit, Shadadi, and soon, Manbij - that were central to its rise; and the coalitionbacked forces arrayed against it are increasingly confident and on offense, with our support.

I have included an annotated map as an attachment to this testimony, which points to our focus areas in the core, and demonstrates that we are now able to apply multiple points of pressure at once, from Manbij, to Fallujah, to Mosul. ISIL is under more pressure than ever before, and we will ensure that it increases dramatically over the coming weeks.

To assess the current situation, I will briefly review eight indicators that we track week-to-week to determine where we may need more focused efforts, and how the campaign is doing overall. These indicators are not exhaustive, but provide a decent top-line overview of what remains an extraordinarily complex, dynamic, and fast-moving situation on the ground.

1. Morale

ISIL's morale is plummeting. We have seen credible reports of ISIL executing its own fighters on the battlefield. Whereas it once claimed to represent the people under its control, it is now

executing anyone seeking to leave its control. Whereas it once massed and maneuvered at will across Iraq and Syria, it can no longer operate in the open, train, or communicate. Whereas it once promised lavish pay for recruits, and free services in its 'caliphate,' it is now slashing pay, cannot provide services, and is facing internal resistance. We know from other sources, as well, that ISIL fighters are panicking on the battlefield, foreign recruits are now looking to return home, and leaders are struggling to maintain discipline, even despite the threat of execution for disobedience.

This picture from the ground level is also apparent in ISIL's own propaganda. Whereas ISIL once promised paradise with staged and sun-drenched scenes from Raqqa and Mosul, ISIL's own leaders now acknowledge they could lose Raqqa and Mosul. ISIL spokesman Muhammad al-Adnani, for example, has for years described ISIL as a global, historic, expanding movement. His catchphrase was 'remain and expand' - describing the territory under its control - and he promised ISIL would someday dominate the Middle East and ultimately control territory in southern Europe. Adnani's latest statement in May was quite different. No longer the confident voice of an expanding movement, he acknowledged that ISIL may lose its holdings in Iraq, Syria, and Libya, including its strongholds of Mosul, Raqqa, and Sirte. We are now working to ensure that his prediction comes true, and that Adnani himself - who also leads ISIL's external operations arm - is eliminated, and no longer able to spew his incitement.

2. Territory

Territory is not the only indicator that matters, but it is significant for three reasons: First, territory, with millions of people under ISIL control, allows ISIL to extract resources, fund external operations, and embed its violent and genocidal system of control, raping women, murdering LGBT individuals, indoctrinating children, and brutally executing anyone who resists.

Second, territory allows ISIL to proclaim itself as vanguard of a historic 'caliphate,' which more than anything else we have seen, drives recruiting from around the world.

Third, and most important, territory and safe haven allow ISIL to plan future operations against our partners, and our own homeland, such as the suicide attacks in Paris, Brussels, and Ankara, which were planned in Raqqa with the support of logistics nodes in and around Manbij.

For all of these reasons, we must pressure ISIL in the areas it

controls, and then take those areas away from ISIL altogether. I have included an attached map to guide the briefing on how and where we are comprehensively shrinking ISIL's territory. The trajectory is positive. ISIL has not had a major battlefield victory in over a year. It has lost 47 percent of its territory in Iraq, and 20 percent in Syria. More important than percentages, however, is the strategic nature of the territory that ISIL has lost: nearly the entire border between Syria and Turkey, iconic cities like Ramadi, Tikrit, and Fallujah, and all the major transit points between Raqqa and Mosul, such as Sinjar, Hawl and Shahdadi (number three and four on the attached map), are no longer controlled by ISIL.

We are now working with local partners to shrink this territory further, through a combination of military, political, and security measures. I will highlight three areas where active ISIL offensives are now underway:

Manbij Pocket

First, is the 'Manbij Pocket,' labeled number one on the map. This has long been the last stretch of territory with access to an international border, allowing foreign fighters to transit in and out of Syria. We commend Turkey for taking measures to tighten the border on the north side, but the threat will not reduce until the territory inside Syria is taken away from ISIL. That is what we are now doing.

Three weeks ago, the Syrian Democratic Forces - a mix of Syrian Kurds, Arabs, Syriac Christians, and Turkmen - launched a surprise attack from the east, crossing the Euphrates River and then rapidly enveloping Manbij city. As we speak, these fighters are now entering the city limits, under cover of coalition air support. ISIL has threatened to kill civilians leaving the city, and ordered a fight to the death. This has only reaffirmed the importance of this operation, which is on track to succeed.

This operation against Manbij was planned for months with military and political components. In my visits to Kobani, Erbil, and Sulaimaniya, I met the leaders of the military alliance now leading the offensive. Named the Manbij Military Council, it is 3,500 strong, over 80 percent Arab, mostly from the local area, fighting to free their own hometowns. This is a core premise of our strategy for liberating territory: we want local people, with local knowledge, in the operations to free their communities from ISIL, and stabilize the areas after ISIL is gone.

It took time to build this inclusive alliance, but the results on the ground, thus far, are promising, and provide a model as we

look to isolate Raqqa - likely the next phase of operations after Manbij - with a predominantly Arab and locally-grown force. The Manbij operation is also proving what we knew going in: that this area was a locus of ISIL's foreign fighter and external plotting network. Of the more than 1,000 ISIL fighters killed in this operation thus far, we believe nearly half are foreign fighters, and we are collecting information along the way on how ISIL's foreign fighter networks are organized and led.

From the other end of the Manbij pocket, we are working with moderate opposition groups to push east across what is known as the 'Mari Line' (the extent of ISIL's westward advance). This effort had struggled - ISIL had the area heavily defended - before we launched the second front across the Euphrates, which pulled ISIL fighters away and allowed our moderate partners to advance.

We will continue to resource both offensives, and we are committed to collapsing ISIL within this pocket, an objective that is central to our own national security. We are also working, in coordination with Turkey, to ensure that local mistrust between elements in both offensives can be overcome, and humanitarian aid can flow into these areas as soon as they are liberated.

Anbar Province

Second, in Iraq's Anbar province, parts of which had been dominated by ISIL for nearly two years, Iraqi security forces and local tribes have recently liberated Ramadi, Hit, central Fallujah, Rutbah, and broke the siege of Haditha, where Sunni tribes held out heroically against ISIL since the summer of 2014. Adnani, the ISIL spokesman, once boasted that Haditha tribes would be wiped off the map, and that fathers would bring their sons to Haditha and say 'this is where the Jughayfa (a leading tribe) once stood.' In fact, Haditha, like Kobani in Syria, broke the back of ISIL and sparked the momentum we are now seeing across Anbar province.

This would not have been possible without local support, and we commend the Government of Iraq and Prime Minister Haidar al Abadi for supporting a program of tribal mobilization in Anbar province. There are now 20,000 Sunni tribal fighters working with Iraqi forces to clear and hold territory, in addition to over 14,000 local police across the province. We have been proud to support this program, together with our coalition partners, at two facilities in Anbar, one on AL Asad airbase near Haditha, and one at Taqadum airbase between Ramadi and Fallujah.

The results are impressive and now must be sustained. We have worked closely with the Government of Iraq to ensure that tribal fighters are embedded into the state security structure, thereby correcting a defect in the Anbar ‘awakening’ model from 2007 and 2008, which was hugely successful, but more ad hoc and sustained with U.S. support. The Iraqis have allocated resources to these new fighters, and woven their ongoing support into their national budget, passed by the Iraqi parliament, thereby helping to ensure ongoing and long-term support.

In Fallujah, Iraqi forces broke through the crust of ISIL's defenses last week and on Sunday announced the full liberation of the city. I was in Iraq last week and met with Anbar's governor, and two months ago met with the most prominent Fallujah sheikhs, all of whom pleaded with us to support their city's liberation. We have been proud to do so, not only with military support, but also with an Italian-led training program for local police to secure the city when military operations cease, a \$100 million nationwide coalition-funded stabilization program to help return people to their homes, a \$20 million allocation in humanitarian aid to reinforce the UN-led effort to manage the flow of Fallujah residents escaping ISIL's brutality, and a comprehensive mine clearance program.

The Fallujah operation has not been perfect. This is among the toughest places to fight in all of Iraq, and ISIL had controlled the city for over 2.5 years. There were concerning reports of abuses against civilians in the early stages of the operation, and the outflow of people initially overwhelmed the UN and humanitarian organizations. This was a primary focus of my visit to Iraq last week, and while we are encouraged by the immediate response to reports of abuse, and the infusion of resources to support IDPs, more must be done, and we have called on all of our coalition partners to help.

Stabilizing areas after ISIL can be even more important than clearing areas from ISIL. We are encouraged that, thus far in the campaign, no significant territory liberated by coalition-backed forces has been reclaimed by ISIL. Anbar is case-in-point: we have focused from the beginning, even when the situation seemed nearly hopeless, on investing local people in their own liberation, pooling coalition resources on stabilization needs, and working with the Government of Iraq to invest local leaders with authority to revitalize populated areas that had been devastated by ISIL.

We are focused now on reopening the Baghdad-Amman highway through Rutbah and the Trebil crossing (number eight on the attached map). This was a key topic of discussion in my meetings last week

with Prime Minister Abadi in Baghdad, and then King Abdullah II in Amman. This highway before ISIL contributed to 20 percent of Jordan's exports and nearly \$100 million per month in trade; thus, reopening it is a main priority to help economically shore up some of our main allies in the region.

We are also working to return people to their homes in Ramadi, a process that has been slowed by ISIL's planting booby traps and improvised explosive devices (IEDs) in civilian homes as well as considerable damage to infrastructure in the city as a result of ISIL's occupation. Tragically, of 60,000 initial returnees, nearly 100 were killed due to bombs planted in their homes, a tactic that once again reveals the lie that ISIL claims to represent the Sunnis of Anbar. In reality, ISIL has been focused on killing Sunnis to gain power, but lost the battle, and littered homes with bombs to keep life from returning to places like Ramadi.

Thanks to coalition contributions, a U.S. company, JANUS, is now overseeing the painstaking work of clearing Ramadi of booby traps, and preparing the ground for stabilization projects. We are aiming to repeat in Ramadi and then in Fallujah what we ultimately saw in Tikrit, where 95 percent of the population has returned to their homes after ISIL. Life there is returning to the streets, with local police in charge, businesses restarting, the university open, and Iraqi-led rebuilding projects underway.

Ninewa and Mosul

All of this sets the stage for what will be the greatest challenge to ISIL as we know it: the liberation of Mosul. For the past six months we have been working with local forces in Iraq and Syria to isolate Mosul from its supply routes in Syria. Operations in Hawl, Shahdadi, and Sinjar, helped cut roadways between Raqqa and Mosul, forcing ISIL leaders onto back roads, where they are easily targeted.

Last week, Iraqi forces began an operation from the south to cut ISIL's access points and sever the connections with areas ISIL still controls, such as the small towns of Hawija and Sharqat in Kirkuk and Salah Ad Din provinces. This operation is now underway and making considerable progress, enabled by Apache helicopters and other accelerants authorized by the President in April.

But Mosul is not simply a military challenge. It is a political, economic, diplomatic, and humanitarian challenge that, if not done right, may well outstrip the capacity of the Iraqi government, and the Kurdistan Regional Government, to manage alone. The only way it can succeed is if everybody - Iraqi

forces, Kurdish Peshmerga, and local fighters from Ninewa - work together as part of a coordinated political-military plan.

I am pleased to report that this is now coming together. Late last year, the Iraqis established a joint headquarters facility at Makhmour, to the southeast of Mosul (near number five on the map). U.S. Marines arrived to support this joint operations center in February, and we tragically lost one of our Marines there in March. These heroic Marines together with our Special Forces advisors have helped Iraqi and Kurdish Peshmerga forces begin to turn the tide south of Mosul, enabling successful operations to seize villages and strategic territory held by ISIL since 2014.

The military advances have finally enabled the political planning that is essential to getting ISIL out of Mosul and stabilizing Mosul after ISIL. Last week, President of the Iraqi Kurdistan Region, Masoud Barzani, held a historic meeting with Iraq's National Security Advisor, Faleh Fayyad, to discuss all aspects of the Mosul campaign. Barzani and Fayyad invited the U.S. to attend, and I was pleased to represent the United States, together with our terrific ambassador, Stu Jones.

This meeting began to solidify planning, to include authorization and funding for 15,000 local fighters from Ninewa to take part in the operation - building on the model that has worked in Anbar - as well as the political arrangements after ISIL.

We are also working through the coalition to ensure resources are ready to support internally displaced persons (IDPs) from Mosul and lay the groundwork for their return and stabilization after ISIL. Next month at the State Department, we will cohost with Canada, Germany, and Japan, a pledging conference to support specific humanitarian and stabilization needs in this regard.

There is a great deal of work left to do, and we will not put a timeline on the Mosul operation. But with momentum now on our side, it is safer to say that ISIL's days in Mosul - where it proclaimed its phony caliphate to the world - are numbered.

Southern Syria

As we squeeze ISIL out of its strongholds in Iraq and Syria, we must remain focused on southern Syria, where it may attempt to fill empty spaces and threaten our partner Jordan. I was in Amman last week, meeting with His Majesty King Abdullah II and his national security team, the day after an ISIL attack killed seven Jordanian soldiers on their border. I expressed our profound condolences for those lost in this attack, and pledged unwavering

support for Jordan and its Armed Forces.

Jordan has done its part in housing nearly 630,000 UN-registered refugees and their capacity has reached a limit. Near the site of the attack last week, approximately 60- 100,000 Syrians are located in a tent city inside Syria across a berm from the Jordanian border. This is not Jordan's problem alone; it is an international problem, and one the international community must work with Jordan urgently to resolve.

We are supporting moderate opposition fighters in this region of southern Syria (number nine on the map) to pressure ISIL and help the defense in-depth of Jordan. These brave fighters have suffered ISIL vehicle bomb attacks, and last week, Russian jets bombed the camp, claiming not to know who was there. We have found Russian explanations of this attack to lack merit, and while there is now a 'no strike' box over the area, the episode once again called into question Russian intentions in Syria.

Finally, we are working to root out an ISIL presence in the SW tri-border region of Syria adjacent to Jordan and the Golan Heights (number ten on the map). ISIL's media statements in recent months, as they suffer losses on the battlefield, have focused on Israel as a target, clearly hoping to generate international headlines to compensate for its defeats. We must not allow this to happen. Last week, I stood at the border, where ISIL positions and training facilities were visible in the distance.

The State Department earlier this month designated the ISIL affiliate in this area, formally known as Yarmouk Martyrs Brigade, as a specially designated global terrorist entity, and we are now working with moderate opposition groups to free Syrians under its grip from their barbaric rule.

We cannot permit ISIL to re-establish a presence anywhere in Syria, let alone on the borders of our closest friends.

3. Combat-Ready Fighters

ISIL's access to fighters has steadily diminished, now at the lowest point we have seen since the summer of 2014. We currently estimate that ISIL fields 18-22,000 overall fighters in Iraq and Syria, the lowest assessed range since we began conducting rigorous reviews of its manpower. This is down from a high-end estimate of 33,000 ISIL fighters in 2014. We are also seeing significant reduction in the flow of foreign fighters entering Syria and Iraq each month, and we are working through our coalition to identify and ensure that ISIL affiliated fighters

cannot travel across borders. In short, we are making it harder for them to travel into Syria, and once there, making sure they can never leave.

This is painstaking work, requiring coordination across borders, and between executive and legislative branches. In September 2014, the President chaired a UN Security Council meeting to adopt the Chapter VII Resolution 2178, which calls on all states to take measures to deter travel of foreign fighters. Since then, our engagement with Middle Eastern and European partners has achieved results through increased informationsharing, better border security, improved counter-terrorism laws, counter-messaging, and improved cooperation between law enforcement and intelligence services.

Since the adoption of UNSCR 2178, more than 40 at risk countries have enacted laws or amendments to enhance obstacles for foreign terrorist fighters traveling into Iraq and Syria. At least 38 countries have reported arresting foreign terrorist fighters or aspirants, and 30 countries have successfully prosecuted foreign terrorist fighters, including the United States. In the United States, my colleagues at Department of Homeland Security and the FBI assess that over 250 U.S. citizens have joined or tried to join ISIL.

We must remain vigilant, here at home, and around the world. The United States now has information-sharing agreements with 55 international partners to assist efforts to identify, track, and deter the travel of suspected terrorists. Equally important, 58 countries, plus the United Nations, now contribute foreign fighter profiles to INTERPOL, and there has been a 500-percent increase in suspected foreign fighter identities in the INTERPOL database. Through our global coalition, we are discussing with INTERPOL how to appropriately incorporate foreign fighter data from the battlefield, ensuring that terrorists who manage to leave Syria can be identified in a routine traffic stop or at border entry, or those who die in Syria can be identified to map domestic contacts.

In addition, The European Union parliament in April issued an EU-wide directive to expand the Passenger Name Record (PNR) database, which would require more systematic collection, use, and retention of data on international airline passengers. This is an important step to ensure the interoperability of data systems across the EU so foreign fighters and terrorists can be tracked in real time, allowing law enforcement, intelligence agencies, and border security to foil ISIL attacks.

4. Access to Revenue

ISIL's revenues are overwhelmingly generated from the territory it controls, primarily from oil extraction and taxation/extortion of local citizens. This picture was not clear when we began the campaign in 2014, but through raids by our Special Operators inside Syria, and incredible work by our unsung intelligence analysts, the U.S. Government has been able to map ISIL's resource stream, and then, systematically, destroy it.

Under Operation Tidal Wave II - which aims to degrade and destroy ISIL's energy assets - the Coalition has carried out precision strikes against oil fields, infrastructure, oil-tanker trucks, banks, and cash storage sites that sustain ISIL's war effort. This phase of the campaign was preceded by many months of planning from across the U.S. Government. We sometimes hear that we just need to 'bomb the oil fields' as if there is a simple military solution to this challenge; in fact, the military effort is the sharp end of the spear, and its success depends on hard-earned intelligence, careful analysis, and target development.

Because we took a systematic approach to this problem, the operations against ISIL's economic infrastructure have been quite successful to date. ISIL was forced to halve fighter salaries in Raqqa and is detaining its own senior officials for trying to steal cash and gold. This has created a virtuous cycle: terrorist fighters are not paid, their supplies run low, they have less will to fight, and they are more easily defeated. Since the strikes against cash storage sites in Mosul, we have seen fighters thin out, with fewer checkpoints, and increasing reports of ISIL leaders executing their own rank-and-file for poor discipline.

This pressure will only increase. Just a couple of weeks ago outside Mosul, coalition strikes destroyed 600 oil transport trucks. Since these strikes began, trucks no longer line up at oil fields, and truck drivers are demanding higher pay to take on the risk of transporting ISIL oil, thereby increasing costs, reducing revenues, and making it even more difficult for ISIL to generate revenue from, or to use, energy resources.

At the same time, we continue to take out ISIL's cash storage sites, destroying their ability to pay fighters and sustain operations. In total, we have conducted more than 120 strikes on ISIL cash centers and oil infrastructure, and this number will continue to rise. We have also worked closely with Coalition partners in the region, particularly the Government of Iraq, to cut off ISIL's access to the international financial system and to disrupt its ability to move and store funds.

ISIL is an adaptive organization, however, and it is working to adapt to this pressure. It is our mission to adapt faster than they do, and continue the relentless pressure across the breadth and width of their operations. We are currently undergoing a careful assessment of ISIL's adaptation to our campaign, and as they adapt, we will respond aggressively.

5. Access to Borders

As noted above, ISIL now controls only a 98-kilometer strip of an international border in Syria, and it is shrinking. The loss of access to this border will deprive ISIL of its only route for material and foreign fighters, as well as degrade its ability to plan and launch external attacks. We know that many of the Paris attackers, for example, entered Turkey from this strip of border, and later flowed northward to Europe. This is unacceptable, and we must make every effort to shut it down these areas entirely to ISIL.

We are also supporting our NATO-ally Turkey on their side of the border to enhance border defense, utilize technology for monitoring, and implement effective systems to eliminate the flow of foreign fighters. It is impossible to seal the border entirely, but we have seen a marked increase in Turkish defenses, and ISIL propaganda has even appealed to its recruits not to travel into Syria, but instead, head to Libya.

They will find an inhospitable welcome in Libya. The Libyans are rejecting ISIL en masse, and what Adnani promised would be another citadel of his self-proclaimed caliphate is facing resistance from GNA-aligned Libyan forces and is now an isolated and shrinking piece of one city on the central coast, Sirte. In the last two weeks alone, multiple offensives by forces aligned with the Libyan Government of National Accord (GNA) advanced rapidly towards Sirte and now have the city surrounded. These fighters have suffered casualties, but they have kept moving forward. If the GNA and Prime Minister Sarraj request support from the international community, and the counter-ISIL coalition, it will find many willing partners. The international community and our global coalition have united in support of the GNA.

6. Capable and Confident Leadership

Two years ago, around this time, I was in Iraq when Abu Bakr al-Baghdadi pronounced the establishment of a 'caliphate' from the largest mosque in Mosul. It was Ramadan, and the announcement, despite being denounced by thousands of Muslim leaders and scholars from around the world, spiked ISIL recruiting and the confidence of its adherents as a historic movement on the march.

Baghdadi and other leaders throughout the summer of 2014 were appearing in the open, speaking, and recruiting.

I just returned from another trip to Iraq. It is Ramadan once again. Yet, we have not heard from the so-called 'Caliph' in more than six months. This Ramadan is being celebrated not by Baghdadi, but by millions of Iraqis taking the streets each night as ISIL and its leaders have retreated to the shadows.

We have no evidence that Baghdadi is dead, but many of his deputies are. We have killed more than 100 mid-to-senior level ISIL leaders in the past few months alone, and the key deputies for Baghdadi in 2014, terrorists known as Abu Sayaf and Hajji Iman, have been killed by U.S. military forces. Baghdadi is not far behind.

In short, whereas ISIL once had leaders exhorting fighters in the open, making public addresses, and mocking the civilized world, its leaders are now dead, or in hiding, and issuing written orders for inexperienced fighters to launch desperate missions against the increasingly confident and capable forces arrayed against them. We will work to make sure these trends continue.

7. Media

As ISIL loses leaders, territory, and resources, its message appears to be having less resonance online. We are countering its message 24/7, with coalition efforts led by UK, UAE, and Malaysia, providing counter-content with localized focus for different regions of the world. I have visited the Sawab ('Right Path') Center in UAE, which is led by smart and energetic young people determined to defeat ISIL in cyberspace, and they are succeeding, with innovative media campaigns focused on ISIL defectors, and the truth behind what ISIL promises versus what it delivers on the ground, especially for women. In the United States, the Global Engagement Center (GEC) coordinates, integrates, and synchronizes government-wide communications activities to counter ISIL's messaging. The GEC also help provide assistance with content development platforms, and amplifying effective voices against the perverse ISIL narrative.

Twitter recently announced that it has eliminated nearly 125,000 ISIL-related or ISIL-affiliated 'handles,' and that number is growing. Facebook and YouTube are similarly removing ISIL-related content from their platforms. Within the coalition, we have widely publicized how anyone can report ISIL content on-line, so that platforms can remove it if the content violates a platform's terms of service, which it often does.

These efforts are having an impact. Pro-ISIL content is down and anti-ISIL content is up. Whereas ISIL two years ago had nearly free rein in cyberspace, today, there are reportedly six people opposing ISIL's message online for each person supporting it. We need these numbers to increase, and recognize that the most effective voices are not governments, but individuals, with their own first-hand accounts of the horror under ISIL rule. As these stories increase, ISIL's message is on defense, and it is our job to help keep it that way.

The Muslim world is also fighting the ideological battle. Shortly after Baghdadi declared himself 'caliph,' 120 Muslim scholars from around the world released an open letter challenging and denouncing ISIL's philosophy. The scholars took ISIL's false claims one-by-one, using evidence directly from the Quran to illustrate how Baghdadi's whims run counter to the teachings of Islam. More and more Muslims are taking to the Internet and public spaces to counter ISIL's brand of hate and take back their faith.

8. Global Branches

From its core in Iraq and Syria, ISIL has declared eight global branches: Libya, Saudi Arabia, Yemen, Sinai, Nigeria, Algeria, the Caucasus, and Afghanistan-Pakistan. We have carefully studied the situation in all of these locations, and in most, a pre-existing terrorist organization, such as Boko Haram, chose to wave the black flag of ISIL. In other cases, such as Yemen, or Afghanistan, small ISIL affiliates have broken off from larger al Qaida movements. We have been actively engaged in these regions, against existing threats, such as AQAP in Yemen, and we should not alter course just because a terrorist group chooses to fly an ISIL flag. Changing flags does not fundamentally change the nature of what - in most cases - was a pre-existing problem, or threat.

Where, however, we see threats emerge anew, or resources directed from the core in Syria to a global branch, it is a concern and we must determine how to act, and act effectively. Libya has been the best example, with ISIL capitalizing on a security vacuum and sending some of its most experienced operators to establish ISIL-Libya. One was named Abu Nabil, a Baghdadi acolyte and experienced terrorist. When we see a leader like this emigrating from the ISIL core to a global branch, we act. Accordingly, Nabil is now dead, targeted with precision in a U.S. airstrike. We have also taken military action to degrade the ISIL network in Libya responsible for launching external attacks in Tunisia.

To root out ISIL-Libya, however, we are building a robust

partnership with the Libyan Government of National Accord (GNA). ISIL's growth in Libya appears to have plateaued in its recruitment of 5,000-8,000 fighters, most from within Africa. Its recruiting drive for European fighters has not succeeded, with numbers in the low hundreds; and for those who made their way to Libya, they may soon lose their stronghold in Sirte.

ISIL-Libya is now under significant pressure. It has been largely expelled from Derna and we have increased engagement with our North African partners to further mitigate the threat, while supporting the UN-led political process in support of the GNA. Just a few months ago there was no government on the ground. Today, the GNA is on the ground in Tripoli, and has aligned forces east and west of Sirte, which are making gains, isolating the city, and forcing many ISIL terrorists to flee. These GNA-aligned forces have demonstrated they are willing and able to fight ISIL, and we are working with Prime Minister Sarraj on an arms embargo exemption request to further support the GNA and our local partners on the ground.

The second branch of concern is Sinai, which we assess was responsible for destroying the civilian Metrojet airliner nine months ago, killing 224 people. I was in Cairo last week discussing the Sinai situation, on the heels of visits by Chairman Dunford and CENTCOM commander General Votel. We are determined to support our Egyptian partners in degrading and ultimately defeating the ISIL branch in Sinai.

The Sinai branch is comprised from a pre-existing violent extremist group, Ansar Bayt alMaqdis. We estimate its manpower to be from several hundred up to 1,000, with some estimates far less than that, and some slightly more. The current situation in Sinai is a low-grade conflict combining links to the ISIL core with violent extremist ideology drawn from Salafist beliefs and long-standing local grievances. The Egyptian Army has increased combat operations and closed almost all the tunnels that facilitated arms smuggling along the Gaza border.

The United States strongly supports Egypt's efforts to combat ISIL-Sinai, a message I conveyed in Cairo last week. We are providing Apache helicopters, MRAPs, counterIED training and border security programs, and have intensified military-to-military discussions on how we can help Egypt adopt the counter-insurgency doctrine and tactics it needs to deal ISIL-Sinai a lasting and permanent defeat.

The Sinai security situation also impacts the Multi-National Force and Observers (MFO) mission. The U.S. is firmly committed to supporting the Treaty of Peace and MFO operations.

Accordingly, we support the MFO's decisions to both modernize operations and implement force reductions that mitigate risk and enable continuation of its mission. Beyond the Sinai and Libya branches, we continue to monitor ISIL's attempts to establish additional ones, such as in the Philippines, Bangladesh and Somalia. We are engaging partners and host nations in a whole-of-government approach to ensure that ISIL cannot grow roots in any of these locations.

Accordingly, while we focus on the core in Iraq and Syria, and cannot be distracted every time a pre-existing terror group waves a black flag, we are working to enhance the capacity of local partners to identify and eliminate emerging threats before they can materialize. This is part of a comprehensive and globally integrated campaign plan to contest ISIL in all dimensions, and stay attuned and ahead of emerging threats.

Looking Ahead

Defeating ISIL in Syria and Iraq (measured by its inability to control significant territory and threaten the viability of the Iraqi state), suffocating its global affiliates, and drying up its global networks, are all achievable objectives. Our strategy is making progress. However, ISIL as a threat, its existence as a cellular terrorist organization, or an appealing banner for disturbed individuals searching for meaning in their lives, will be with us for many years.

To further mitigate the threat, we are focused as much on what comes after ISIL, as we are on defeating ISIL. In Iraq, the coalition is providing resources to alleviate human suffering and help return people to their homes (over 725,000 to date), strengthen inclusive local governance, address macro-economic risks, and stabilize local communities through an innovative funding mechanism that is delivering results. Ultimately, however, long-term stability in Iraq rests on the Iraqis, and the center of all communities, Sunni, Shia, and Kurd, must hold against extremes working to pull the country - and their communities - apart.

That center is stronger now than it has been in two years, but the situation remains fragile and volatile. U.S. engagement remains vital.

It will also be important to support the Government of Iraq in reforming security institutions after ISIL, managing the demobilization of volunteer forces, and ensuring that the state has full control over armed groups, which must operate under an agreed legal framework.

In Syria, as ISIL is losing territory in the east, its terrorist rival - Jabhat al-Nusra - is gaining ground in the west, putting down roots in Idlib province along the Turkish border. Nusra is establishing schools and training camps, recruiting from abroad, launching major military operations, and enjoying a sophisticated on-line presence, all the while providing safe haven for some of al Qaida's most experienced terrorists. With direct ties to Ayman al Zawahiri, Osama Bin Laden's successor, Nusra is now al Qaida largest formal affiliate in history.

This is a serious concern, and where we see Nusra planning external attacks, we will not hesitate to act. To end Nusra as a threat, however, we must find a mechanism to de-escalate and end the Syrian civil war, thereby allowing the moderate opposition to take charge of its own territory, without threat of Asad's barrel bombs overhead, or terrorists down the street. As the war goes on, the opposition is increasingly interwoven with Nusra, which provides pretext for the criminal Asad regime to target anyone it wants, on grounds that it is targeting terrorists. Nobody is fooled by this argument.

At bottom, the Syrian civil war remains an incubator for violent extremism, and to defeat the threats against our homeland over the long-term, we must find a diplomatic mechanism to enforce a nationwide cessation of hostilities, thereby isolating Nusra from the opposition, concentrating efforts on ISIL, ending bombardments by the Asad regime, and, ultimately, facilitating the political transition called for in UNSCR 2254 and the International Syria Support Group.

Conclusion

It is once again an honor to appear before this Committee. Our global campaign against ISIL is making progress and will accelerate over the coming weeks. This does not, however, mean the threat of terrorism will end. It will require constant collaboration with Congress to stay ahead of this most dynamic and complex challenge. I look forward to your questions.

BRETT H. MCGURK
Special Presidential Envoy
Global Coalition to Counter Isil

DEFENDANTS' EXHIBIT 164:

2016 WL 3627191
Roll Call, Inc.
Copyright (c) 2016 CQ-Roll Call, Inc.

Testimony
July 06, 2016

Senate
Homeland Security and Governmental Affairs
Investigations
Countering Terrorist Internet Recruitment

Opening Statement of Rob Portman
Chairman
Subcommittee on Investigations

Committee on Senate Homeland Security and Governmental Affairs
Subcommittee on Investigations

July 6, 2016

This hearing will come to order.

When the Subcommittee began planning this hearing, we did not know it would fall just three weeks after the most deadly terrorist attack on American soil since September 11, 2001. The evil terrorist attack in Orlando last month that targeted the LGBT community was yet another reminder of the urgent need to reexamine and redouble our government's efforts to combat violent Islamic jihadism both at home and abroad - and particularly to disrupt and ultimately destroy the so-called Islamic State of Iraq and Syria or ISIS. There is no room for complacency on this issue. It warrants continuous scrutiny and oversight from Congress as our government's understanding of the enemy evolves.

ISIS specializes in savagery-violence inspired by delusions of sectarian conquest from another age. Yet it has effectively deployed modern technology of the information age to spread its propaganda and recruit killers to its cause. ISIS has developed a sophisticated information warfare capability. It has pioneered a distinctive strategy of targeted online recruitment, while disseminating sleek viral videos and messages, primarily from two media centers, al-Hayat and al-Furqan through a constantly evolving set of online platforms.

As FBI Director James Comey has noted, even if we are able to keep foreign terrorists physically out of the United States,

online communication and social media allow ISIS to ‘enter as a photon and radicalize somebody in Wichita, Kansas.’ ISIS has weaponized online propaganda in a new and lethal way.

The damage wrought by that weapon is considerable. Orlando-49 dead. San Bernardino-14 dead. Fort Hood-13 dead. The Boston Marathon-3 dead and hundreds wounded. Each of these killers was reportedly radicalized to some degree by online jihadist content. And so many other attacks inspired by means of social media have been thwarted.

Indeed, experts tell us that throughout last year, social media played some part in radicalization of all 60 people arrested in the United States for criminal acts in support of ISIS. Most recently, of course, the FBI has publicly stated that it is ‘highly confident’ that the Orlando killer Omar Mateen was ‘radicalized at least in part through the Internet.’

One longstanding aim of the ISIS propaganda machine is to attract foreign fighters to ISIS-controlled territory. Often ISIS tells its recruits tales of high adventure, joined with false narratives of an Islamic extremist utopia. The bizarre images behind me, for example, appear in a ISIS film exhorting Muslims around the world to join the Islamic State; rather than show ISIS fighters for what they are - murderers of innocent victims who are themselves overwhelmingly Muslim - they are shown playing with laughing children and shopping in local marketplaces. Appeals like these have helped draw an estimated 30,000 foreign fighters, including at least 6,000 Westerners, to take up arms with ISIS.

The good news is that the Defense Department reports a significant decrease in the flow of foreign fighters to ISIS territory. At the same time, however, ISIS has increasingly shifted its propaganda efforts to inciting sympathizers to commit acts of terror in the West-including in the United States.

Online propaganda, amplified by social media and peer-to-peer communication, is now a key weapon in ISIS's arsenal. We should, of course, resist over-simplifying the problem. Not all radicalization in the United States occurs online, and in-person interaction often reinforces the process. But unlike the more common European pattern of jihadist radicalization in clusters or in prison, the U.S. threat so far is predominantly that of the lone wolf terrorist-an individual radicalized on his own, often in front of his computer screen with access to online jihadist content and videos that create a kind of virtual training camp.

In addition to a clear military strategy and vigilant law

enforcement efforts here at home, the United States and our allies need a more robust, coordinated strategy to expose the enemy's lies, counter its false narratives, and encourage credible voices to tell the truth to those most susceptible or receptive to ISIS's lies.

And that is true both of foreign and U.S. audiences. Although the ISIS online radicalization threat is well-recognized, there is a range of opinion on how best to combat it, and U.S. government efforts are still in early stages. Today we will examine the counter-messaging initiatives that show promise-and where the U.S. government has fallen short and could accelerate its efforts.

In January, the State Department began a revamp of its counterterrorism messaging and coordination efforts with the launch of the Global Engagement Center-a better funded and (at least on paper) more empowered version of its predecessor, the Center for Strategic Counterterrorism Communications. Previous efforts to address this threat have struggled to overcome bureaucratic hurdles, unclear authorities, and a lack of interagency communication and unity of effort. These structural deficiencies will continue to hinder future administrations-both Republican and Democrat-unless they are addressed.

That is why I recently introduced legislation with Senator Murphy to help resolve some of these issues and the impact they have on our ability not only to counter propaganda and disinformation from extremist groups like ISIS but also the equally pressing challenges posed by state-sponsored propaganda from countries like Russia and China.

The Department of Homeland Security also recently consolidated its countering-violent-extremism or CVE efforts in a new Office of Community Partnerships. We'll be hearing more about those efforts in our first panel today, and I will be interested in exploring whether these initiatives are backed by sufficient authorities and resources.

In addition, social media firms including Facebook and Twitter have stepped up their voluntary efforts to police their own terms of service, which prohibit incitements to terrorism. Twitter has closed more than 100,000 ISIS-linked accounts, and Facebook has actively worked to remove offending users while working in various ways to promote content to counter jihadist propaganda. Those actions have helped to degrade ISIS's social media megaphone, according to the Middle East Media Research Institute, but its online presence remains strong.

Let's be very clear: To defeat ISIS, it is necessary to destroy the enemy where they live and prosper - in Iraq and Syria, and in their major cells around the world. Online counter-messaging is no substitute for a clearly defined and vigorously executed military strategy. But a military strategy must be reinforced by a coordinated effort to undermine and disrupt the powerful disinformation spread by Islamic jihadists. Today, we will be hearing from three federal agencies involved in that effort, as well as a distinguished panel of experts who have been engaged on these issues for many years.

With that, I will turn to Senator McCaskill for her opening statement.

ROB PORTMAN
Chairman
Subcommittee on Investigations

End of Document

© 2022 Thomson Reuters. No claim to original U.S. Government Works.

DEFENDANTS' EXHIBIT 165:

FORBES > INNOVATION > CONSUMER TECH

Twitter suspends 'Gateway Pundit' Jim Hoft

AJ Dellinger Contributor ⓘ

I am a freelance technology reporter and editor.

Follow

Feb 6, 2021, 07:18pm EST

Listen to article 3 minutes

🕒 This article is more than 2 years old.



ASSOCIATED PRESS

Jim Hoft, founder and editor of the far-right publication The Gateway Pundit, was suspended from Twitter Saturday evening for

violating the platform's rules. The account, @gatewaypundit, no longer has a presence on Twitter, save for a message that indicates the account has been suspended. Prior to the suspension, the @gatewaypundit account had [more than 375,000 followers](#).

A spokesperson for Twitter said, "The account was permanently suspended for repeated violations of our [civic integrity policy](#)." The policy restricts users on the platform from sharing information that undermines elections and other civic processes, including sharing misinformation regarding the outcome of elections.

Hoft and his publication have been widely criticized for spreading false information, including promoting conspiracy theories regarding the outcome of the 2020 presidential election. A recent study published by [The German Marshall Fund of the United States](#) found that The Gateway Pundit was the leading single source of misinformation shared by verified accounts on Twitter in 2020. In 2019, Wikipedia [deprecated The Gateway Pundit](#), removing its qualifications to serve as a source of legitimate information. The community cited "falsehoods, conspiracy theories, and intentionally misleading stories" that appear on The Gateway Pundit as the reason for the decision.

Recently, Hoft's publication came under fire for sharing a video that it claimed contained proof of voter fraud being committed in Detroit. The video purported to show the delivery of absentee ballots several hours after the deadline for those ballots to be received. The report has already been [widely debunked](#) by local publications in Detroit.

The Gateway Pundit has previously been criticized for [spreading misinformation](#), including [falsely identifying the perpetrators of mass shootings](#), [promoting conspiracy theories about school](#)

shooting events, made false claims about voter fraud and election tampering.

MORE FOR YOU

Why The Rock's Social Media Muscle Made Him Hollywood's Highest-Paid Actor

White House ‘Will Fight’ Texas Court Blocking Abortion Pill—DOJ Will Appeal

Entrepreneurs, Stop Building And Chasing Weak Business Models. Do This Instead

The @gatewaypundit account did not appear to be particularly active on Twitter, per an [archived version of the account](#). The account had not tweeted since January 29. Recently shared content included a mix of retweets that railed against coronavirus restrictions in restaurants and claims that votes cast for President Joe Biden were illegal. Hoft recently shared links to his accounts on alternative platforms, including those associated with the far-right like Gab, Telegram, MeWe, and Minds.

TransformationalTech: Invest in the Future Today

Email address

Sign Up

You may opt out any time. By signing up for this newsletter, you agree to the Terms and Conditions and Privacy Policy

At the time of publication, Hoft had not yet addressed the suspension on any platform.

Hoft was also [photographed in attendance](#) at former President Donald Trump’s “Save America” Rally on January 6. That event occurred just before some in attendance stormed the Capitol, an

event that resulted in the death of five people including one police officer.



AJ Dellinger

Follow

I'm a freelance reporter and editor with nearly a decade of experience covering all aspects of tech. I joined the Daily Dot in 2014 to... **Read More**

[Editorial Standards](#)

[Reprints & Permissions](#)

ADVERTISEMENT

DEFENDANTS' EXHIBIT 166:

White House says social media companies have 'responsibility' to manage platforms amid leaked document fallout

[H thehill.com/homenews/administration/3948542-white-house-says-social-media-companies-have-responsibility-to-manage-platforms-amid-leaked-document-fallout/](https://thehill.com/homenews/administration/3948542-white-house-says-social-media-companies-have-responsibility-to-manage-platforms-amid-leaked-document-fallout/)

Brett Samuels

April 13, 2023



Administration

by Brett Samuels - 04/13/23 10:06 AM ET



Greg Nash

White House press secretary Karine Jean-Pierre addresses reporters during the daily briefing at the White House on Friday, March 10, 2023.

White House press secretary Karine Jean-Pierre on Thursday said social media companies have a “responsibility” to manage their platforms to avoid the spread of material that could damage national security amid the fallout of sensitive leaked documents that circulated on Discord, Twitter and other platforms.

“We do believe that social media companies have a responsibility to their users and to the country to manage the private sector infrastructure that they create and now operate,” Jean-Pierre told reporters in Ireland, where President Biden is visiting for a few days “So we do believe that they have a responsibility.”

She added that “we normally urge companies to avoid facilitating those circulation of material detrimental to public safety and national security.”

Late last week, a batch of classified documents that detailed U.S. briefing materials and were marked “secret” appeared on social media platforms, including Twitter and Telegram

The documents show details on the U.S. assessment of the war in Ukraine, including plans for building up the Ukrainian military ahead of a planned counteroffensive, as well as insight into Russian military planning.

The leaks also include sensitive material on Canada, China, Israel and South Korea, among other nations

The Department of Defense is reviewing the scope of the leak, and the Justice Department is leading an investigation into the source

The White House has not yet confirmed the veracity of the documents, saying that at least some of them appear to be doctored.

Biden on Thursday said the administration is getting closer to determining the source, and he downplayed the severity of the fallout from the leaks.

“I’m concerned that it happened, but there’s nothing contemporaneous that I’m aware of that is of great consequence,” he said.

Tags

Copyright 2023 Nexstar Media Inc. All rights reserved. This material may not be published, broadcast, rewritten, or redistributed.

More Administration News

[See All](#)



[In The Know](#)

Jill Biden urges regular health screenings: ‘I got cancer in a routine checkup’

by [Judy Kurtz](#) 58 mins ago

[In The Know](#) / 58 mins ago



Administration

Biden administration urges return to office for federal workers

by Nick Robertson 2 hours ago

Administration / 2 hours ago



Blog Briefing Room

Jill Biden calls Ukraine's first lady 'the heart of a nation at war'

by Rachel Scully 17 hours ago

Blog Briefing Room / 17 hours ago



Administration

White House blasts 'extreme and dangerous' Florida abortion bill

by [Brett Samuels](#) 18 hours ago
[Administration](#) / 18 hours ago
[See All](#)

Top Stories

See All



[Senate](#)

Dianne Feinstein faces down Democratic firestorm

by [Al Weaver](#) and [Mychael Schnell](#) 6 hours ago
[Senate](#) / 6 hours ago



[Campaign](#)

2024 Republicans descend upon NRA convention under shadow of mass shootings

by [Caroline Vakil](#) 5 hours ago
[Campaign](#) / 5 hours ago



[House](#)

Pelosi seeks balance in post-Speakership role

by [Mike Lillis](#) and [Mychael Schnell](#) 5 hours ago

[House](#) / 5 hours ago



[Court Battles](#)

Biden administration, drugmaker asks Supreme Court to pause abortion pill restrictions

by [Nathaniel Weixel](#) 26 mins ago

[Court Battles](#) / 26 mins ago

[See All](#)

DEFENDANTS' EXHIBIT 167:

**IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF LOUISIANA**

The State of Missouri, *et al.*,

Plaintiffs,

v.

President Joseph R. Biden, Jr., in his official
capacity as President of the United States of
America, *et al.*,

Defendants.

Civil Action No. 22-cv-1213

DECLARATION OF BRANDON WALES

I, Brandon Wales, declare the following, based upon my personal knowledge, information acquired by me in the course of performing my official duties, and information contained in the records of the Cybersecurity and Infrastructure Security Agency (CISA):

1. I am the Executive Director at CISA, U.S. Department of Homeland Security (DHS), serving as the senior career executive helping oversee execution of CISA operations. I am responsible for leading long-term strategy development, managing CISA-wide policy initiatives and ensuring effective operational collaboration across the Agency. I have been with DHS since 2005, and with CISA since it was established in 2018.

I. CISA's Mission

2. As the nation's cyber defense agency, CISA is charged with leading the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure. 6 U.S.C. § 652. Securing the nation's critical infrastructure is a shared responsibility requiring not just a whole-of-government, but a whole-of-nation approach. CISA is only able to accomplish its

mission by building collaborative, trusted partnerships across all levels and branches of government, and with the private sector, academia, and international community.

3. As part of this mission, CISA plays two key operational roles. First, CISA is the operational lead for federal cybersecurity, in close partnership with federal partners. Second, CISA serves as the National Coordinator for critical infrastructure security and resilience, including cybersecurity, working with partners across government and industry to protect and defend the nation's critical infrastructure.¹

4. In relation to its cybersecurity mission, CISA builds the national capacity to defend against "malicious cyber activity" and works with federal partners and provides them with cybersecurity tools, incident response services, and assessment capabilities to safeguard Federal Civilian Executive Branch (FCEB) networks that support our nation's essential operations. CISA strengthens the nation's cyber defense by leading asset response for significant cyber incidents and ensuring that timely and actionable information about known cyber threats and incidents is shared with federal and state, local, territorial, and tribal (SLTT) officials, as well as our international and private sector partners, to ensure the security and resilience of our critical infrastructure.

5. The malicious cyber activity described in this declaration broadly includes threats to the confidentiality (secrecy), integrity (authenticity against alteration), and availability (consistent functionality) of information systems and the information contained therein. Such threats include malware, phishing, exploitation of software vulnerabilities, and other tactics, techniques, and procedures (TTPs).

¹ 42 U.S.C. § 5195c defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

6. Malicious cyber activity, as discussed in this declaration, relates only to unauthorized access to information systems and is distinct from the concept of mis-, dis-, and mal-information, which relates to the veracity and intent behind certain information.

7. Malicious cyber activity is carried out by a variety of actors, including financially motivated criminals and the military and intelligence services of foreign nations (nation-state actors). Such nation-state actors seek to compromise U.S. networks in order to further their geopolitical objectives at the expense of the United States. These policy objectives may include theft of U.S. trade secrets for economic purposes, theft of information for espionage purposes, theft of information to enable separate espionage efforts (*e.g.*, blackmail), or even possibly launching a destructive cyberattack in order to retaliate against U.S. foreign policy decisions, such as the imposition of economic sanctions. See <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/> (last visited April 24, 2023). CISA's efforts to counter malicious cyber activity are largely directed at securing U.S. networks in order to frustrate the efforts of these nation-state actors to achieve their objectives, as well as to frustrate the efforts of criminal gangs that use ransomware to disrupt critical infrastructure systems.

8. With respect to its infrastructure security mission, CISA enhances the protection of critical infrastructure from physical and cyber threats through enabling risk-informed decision-making by owners and operators of critical infrastructure. Activities include conducting vulnerability assessments, facilitating exercises, and providing training and technical assistance nationwide.

9. There are 16 critical infrastructure sectors whose “systems and assets, whether physical or virtual, [are] so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters,” as established by Presidential Policy Directive (PPD) 21. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil/> (last visited April 24, 2023).

10. PPD 21 designates a Sector Risk Management Agency (SRMA) within the federal government for each sector given that agency’s specialized knowledge and expertise with respect to the sector. *See* 6 U.S.C. § 652a(c)(3) (stating that any reference to a “Sector-Specific Agency” in any document of the United States shall be deemed to be a reference to an SRMA).

11. DHS serves as the SRMA for eight sectors and co-SRMA for an additional two sectors, and CISA performs the SMRA function on behalf of DHS for eight sectors. To manage risks to these critical infrastructure sectors, CISA works collaboratively with state and local governments, federal partners, and private sector partners. Furthermore, all other SRMAs must coordinate their activities with CISA. 6 U.S.C. § 665d.

12. CISA has a statutory obligation to “provid[e] shared situational awareness to enable real-time, integrated, and operational actions across the Federal Government and non-Federal entities to address cybersecurity risks,” “shar[e] cyber threat indicators, defensive measures, and . . . other information related to cybersecurity risks and incidents with Federal and non-Federal entities,” and “carry out cybersecurity [and] infrastructure security . . . stakeholder outreach and engagement.” 6 U.S.C. §§ 659(c)(2) and (9); 6 U.S.C. § 652(c)(10). Furthermore, these obligations also extend to CISA receiving, analyzing, and using information to address security risks. For

example, longstanding statutory authorities require CISA to “access, receive, and analyze law enforcement information, intelligence information, and other information from . . . private sector entities, . . . in order to—(i) identify and assess the nature and scope of terrorist threats to the homeland.” 6 U.S.C. § 652(e)(1)(A). That statute imposes a responsibility to maintain “real-time awareness of threats, vulnerabilities, mitigations, and other actions related to the security [of critical infrastructure] sectors.” 6 U.S.C. § 665d(c)(4)(C).

13. In addition to sharing cyber threat, risk, and vulnerability information with federal and non-federal entities, CISA operates an office for joint cyber planning that develops plans for cyber defense operations. 6 U.S.C. § 665b. In 2021, CISA launched the Joint Cyber Defense Collaborative (JCDC) to operationalize this authority and others. The JCDC is a CISA-led effort that includes numerous federal agencies and private technology companies and seeks to counter malicious cyber activity through joint cyber defense operations and closely coordinated operational collaboration.

14. The majority of internet connected devices and critical infrastructure is owned and operated by the private sector. *See* GAO-22-104279, *Critical Infrastructure Protection: CISA Should Improve Priority Setting, Stakeholder Involvement, and Threat Information Sharing* (March 2022).

15. Improving the nation’s cyber and critical infrastructure security therefore necessarily requires that CISA communicate and coordinate with a diverse set of partners, including federal departments and agencies, SLTT governments, academia, and private sector organizations, including technology companies.

16. To carry out its statutorily mandated duties, CISA brings together industry and government organizations to improve information sharing, planning and response efforts for large-scale cyber events, and collaboration on enhanced cyber threat guidance.

17. Under CISA's voluntary information sharing authorities, CISA works directly with victims of nation-state actor and cybercrime intrusions, collaborates with global cloud computing and software vendors who have critical insights into malicious cyber campaigns and activity, coordinates with software vendors on product security, and creates communities that drive down risk for American and global infrastructure.

18. CISA's voluntary collaboration with private industry and government organizations has contributed significantly to the protection of critical infrastructure and the safety of the American people. Public-private collaboration provides critical visibility into cyber threat actor activity, enables cyber defenders to pre-empt or respond to cyber intrusions, and is paramount to mitigating major cyber vulnerabilities and compromises. For example, when a critical vulnerability was discovered in Log4j, an open-source logging framework incorporated into hundreds of software packages used worldwide by countless entities, public-private collaboration led by CISA spurred the development and sharing of effective detection guidance and helped identify impacted products and versions with integrated Log4j software for accelerated mitigation. This collaboration drastically reduced the impact of the Log4j vulnerability by raising awareness and allowing cyber defenders to focus on the most impactful actions to mitigate threats to their organizations. See <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance> (last visited April 24, 2023); <https://www.wsj.com/articles/what-is-the-log4j-vulnerability-11639446180> (last visited April 24, 2023).

19. Other examples of how these collaborative partnerships have demonstrated benefits for U.S. national security include advancing efforts to build resilience against ransomware and increased insight and information sharing into advanced persistent threat (a sophisticated actor that seeks to gain undetected access to computer networks and systems for a prolonged period of time for the purpose of stealing sensitive data or impeding critical aspects of an organization) activity against government and U.S. critical infrastructure owners and operators. *See* <https://www.cisa.gov/news-events/alerts/2022/02/28/broadcom-software-discloses-apt-actors-deploying-daxin-malware-global> (last visited April 24, 2023); <https://www.cisa.gov/news-events/news/readout-second-joint-ransomware-task-force-meeting> (last visited April 24, 2023).

20. In addition to statutory mandates to communicate and coordinate with these various stakeholders, Congress has established advisory committees, such as the Cybersecurity Advisory Committee (the CSAC) to “advise, consult with, report to, and make recommendations to the Director” of CISA. 6 U.S.C. § 665e. Congress has set requirements as to the composition of the CSAC, to include representatives from government and “a broad range of industries.” *Id.*

21. Regular communication and coordination with these stakeholders is, as a result, not only necessary to effectuate CISA’s mission of securing the nation’s cyber and critical infrastructure, but also required by law.

22. Given the whole-of-nation approach necessary to secure our cyberspace and critical infrastructure, CISA publishes accurate information for our partners, stakeholders and the general public, including, for example, cybersecurity alerts and advisories, cybersecurity guidance designed for a variety of audiences from the general public to K-12 schools to small businesses, and the Election Security Rumor vs. Reality webpage. *See, e.g.,* <https://www.cisa.gov/news-events/cybersecurity-advisories> (last visited April 24, 2023); <https://www.cisa.gov/MFA> (last

visited April 24, 2023); <https://www.cisa.gov/protecting-our-future-cybersecurity-k-12> (last visited April 24, 2023); <https://www.cisa.gov/cyber-guidance-small-businesses> (last visited April 24, 2023); <https://www.cisa.gov/rumor-vs-reality> (last visited April 24, 2023).

II. How Cyber Threat Actors Use Social Media Platforms

23. Cyber threat actors often use social media platforms as a mechanism to deliver malware or phishing communications, to send command-and-control instructions to victim computers that the cyber threat actor has compromised through other means, or to carry out other steps related to malicious cyber activity. *See* <https://www.bleepingcomputer.com/news/security/russian-state-hackers-use-britney-spears-instagram-posts-to-control-malware/> (use of comments on Britney Spears' Instagram photos to deliver command-and-control instructions to backdoor trojan) (last visited April 24, 2023); https://www.trendmicro.com/en_us/research/19/d/new-version-of-xloader-that-disguises-as-android-apps-and-an-ios-profile-holds-new-links-to-fakespy.html (use of Twitter usernames, Instagram, and Tumblr to encode command-and-control addresses used by malicious Android application) (last visited April 24, 2023); <https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf> (detailing malware that “uses Twitter, GitHub, and cloud storage services to relay commands and extract data from compromised networks”) (last visited April 24, 2023); <https://www.cyberdefensemagazine.com/astaroth-trojan-leverages-facebook-and-youtube-to-avoid-detection/> (use of YouTube and Facebook profiles to host and maintain command-and-control configuration data, “allow[ing] the attackers to bypass content filtering and other network security measures”) (last visited April 24, 2023).

24. According to the Mitre ATT&CK Framework, an industry-standard cybersecurity taxonomy for describing malicious cyber threat TTPs, cyber threat actors favor this technique

because “[u]sing common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide [from network defenders] in expected noise” that appears in network traffic.

<https://attack.mitre.org/techniques/T1583/006/> (last visited April 24, 2023).

25. When social media companies become aware of malicious cyber activity delivered through their services, they generally block or take down the offending content. *See also* 6 U.S.C. § 1503(a), (b) (authorizing private entities to monitor their information systems and apply defensive measures for cybersecurity purposes notwithstanding any other provision of law).

26. Thus, CISA shares cyber threat indicators or adversary TTPs with technology companies, including social media platforms, in part, to enable them to detect, prevent, and mitigate malicious cyber activity. In order to prevent and mitigate such malicious cyber activity, the private company would typically remove, suppress, or block the content that presents a cyber threat.

III. Potential Harm Caused by the Injunction

27. I am aware that Plaintiffs in this action have asked for the following relief:

The Court should enter a preliminary injunction preventing Defendants, and their agents, officers, employees, contractors and all those acting in concert with them, from taking any steps to demand, urge, encourage, pressure, coerce, deceive, collude with, or otherwise induce any social-media company or platform for online speech, or any employee, officer, or agent of any such company or platform, to censor, suppress, remove, de-platform, suspend, shadow-ban, de-boost, deamplify, issue strikes against, restrict access to, demonetize, or take any similar adverse action against any speaker, content, or viewpoint expressed on social media. The Court should also preliminarily enjoin Defendants from acting in concert with any others, including but not limited to persons and entities associated with the Center for Internet Security, the Election Integrity Partnership, and the Virality Project, to engage in the aforementioned conduct, and from acting in concert with any such others who are engaged in any of the aforementioned conduct.

28. As described in the examples below, Plaintiffs’ proposed injunction could, if interpreted as broadly as plaintiffs seem to suggest, significantly harm CISA’s ability to perform

its statutorily mandated work, which would leave the nation's cyber and critical infrastructure vulnerable.

a. The injunction could be construed to preclude CISA from publishing publish accurate information about any topic—from cybersecurity to critical infrastructure security and resilience—should it lead a social media platform to engage in any “conduct” that is “[m]entioned” in the proposed injunction based on this publicly available information. Given that securing the nation's critical infrastructure is a shared responsibility requiring a whole-of-nation approach, CISA publishes accurate information in countless resources, including, for example, cybersecurity alerts and advisories, cybersecurity guidance designed for a variety of audiences from the general public to K-12 schools to small businesses, and the Election Security Rumor vs. Reality webpage—a webpage that I understand Plaintiffs are offering as evidence in support of their preliminary injunction motion. *See, e.g.*, <https://www.cisa.gov/news-events/cybersecurity-advisories> (last visited April 24, 2023); <https://www.cisa.gov/MFA> (last visited April 24, 2023); <https://www.cisa.gov/protecting-our-future-cybersecurity-k-12> (last visited April 24, 2023); <https://www.cisa.gov/cyber-guidance-small-businesses> (last visited April 24, 2023); <https://www.cisa.gov/rumor-vs-reality> (last visited April 24, 2023). Under Plaintiffs' broad theory of what constitutes encouragement of social media platforms, CISA would be unable to publish any of its resources without running the risk that: (a) a social media company might use those resources in making content moderation decisions, regardless of CISA's awareness that a social media company used that resource; and (b) CISA might be held in contempt of court for running afoul of the injunction.

b. The injunction could also be construed to prevent CISA from sharing cyber threat indicators and adversary TTPs with technology companies, including social media platforms, to enable them to detect, prevent, and mitigate malicious cyber activity should it lead the technology or social media company to independently remove, suppress, or block threatening content to prevent or mitigate malicious cyber activity. Currently, CISA shares an enormous amount of such information. For example, through CISA's Automated Indicator Sharing (AIS) program, CISA has shared 14,000 unique indicators thus far in 2023, enabling recipient organizations—many of which are cybersecurity companies who serve their own customers—to detect, prevent, and mitigate malicious cyber activity associated with these indicators. In addition to AIS, which shares indicators in a machine-to-machine format, CISA also shares cyber threat information through other channels, and CISA's out-bound sharing of indicators spurs in-bound receipt of actionable cyber threat information. Between April 2022 and April 2023, CISA received approximately 300 unique and non-public pieces of cyber threat information, including early warnings that ransomware gangs had obtained access to certain U.S. company networks and were preparing to exfiltrate or encrypt data and hold it for ransom. *See* <https://www.cisa.gov/news-events/news/getting-ahead-ransomware-epidemic-cisas-pre-ransomware-notifications-help-organizations-stop-attacks> (“[S]ince the start of 2023, [CISA has] notified over 60 entities across the energy, healthcare, water/wastewater, education, and other sectors about potential pre-ransomware intrusions . . . many of them identified and remediated the intrusion before encryption or exfiltration occurred.”) (last visited April 24, 2023). If the injunction were construed to prevent CISA from engaging with technology companies, including social media platforms, to address these cyber

threats, such cyber threats would be more likely to remain undetected for longer periods of time, resulting in additional victims being compromised before the malicious cyber threat is discovered, which would present a greater threat to national security.

c. The injunction could also be read to prevent CISA from responding to cybersecurity incidents involving a technology company, including social media platforms or file-hosting sites, because CISA's engagement with the company could be construed as an effort by CISA to “induce” the company to remove malicious cyber content. For example, in March 2023, a sophisticated cyber threat actor executed a supply chain compromise on a Voice over Internet Protocol (VoIP) company. This supply chain compromise caused the VoIP company to unknowingly distribute an altered version of its desktop application to hundreds of thousands of its customers. *See* <https://arstechnica.com/information-technology/2023/03/massive-supply-chain-attack-with-ties-to-north-korea-hits-users-of-3cx-voice-app/> (last visited April 24, 2023). That altered desktop application would then initiate a connection to GitHub—a site owned by Microsoft that allows individual users to develop, host, and download software, and additionally contains significant social features that allow users to comment on or contribute to one another’s work²—in order to download a file containing a list of Uniform Resource Locators (URLs) hosting various types of malware. The altered desktop application would then use the URL list to download the malware, furthering the compromise of the victim’s computer. This type of multi-stage malware delivery is not uncommon, especially for software supply chain compromises. Here, CISA contacted

² GitHub is not the only file-hosting service with social features that cyber threat actors use in furtherance of malicious cyber activity and that may be considered a social media platform, depending on how it is defined. CISA has encountered numerous examples of malicious cyber actors relying on widely-used services like Google Drive, Box, and Dropbox to host malware, deliver malicious communications, and remotely manage compromised victim systems.

GitHub through the JCDC in order to learn about whether this malicious file remained accessible and to help determine impacts to federal entities, which would help illustrate the scope and impact of the incident. Under Plaintiffs' proposed injunction, such engagement with GitHub may be precluded if the Court were to determine that CISA played any role in "induc[ing]" GitHub to remove or otherwise make inaccessible the malicious file.

d. The injunction could likewise be understood to prohibit CISA from notifying or providing a service to notify technology companies of profiles or websites that impersonate federal government agencies or contain other cyber threats, should such notifications or service result in technology companies, including social media platforms, taking any action against them. Such profiles or websites may be used to directly host malicious files, induce users to click links to third-party links that automatically engage in malicious cyber activity, or otherwise defraud users who believe these profiles to be legitimate. In furtherance of CISA's responsibility to secure FCEB systems and in order to maintain the trustworthiness of legitimate FCEB social media profiles and websites and protect the public from malicious cyber activity, CISA may notify technology companies of such information. In addition, CISA provides a no-cost shared cybersecurity service to the FCEB agencies and state fusion centers³ to leverage an IT security company to provide domain mitigation services. Through this service, eligible users can report websites that, among other things, impersonate federal government agencies or malicious cyber activity hosted on a domain to an information technology (IT) security company, and after investigating the reported information, the IT security company may request that the

³ Fusion Centers are state-owned and operated centers that serve as focal points in states and major urban areas for the receipt, analysis, gathering and sharing of threat-related information between SLTT, federal and private sector partners. <https://www.dhs.gov/fusion-centers> (last visited April 24, 2023).

entities that host the domain (*e.g.*, internet service providers, domain registrars, web hosting providers) mitigate the cyber threat, which frequently includes the service provider removing the malicious content. For example, a fusion center in Missouri has taken advantage of the no-cost shared cybersecurity service to report such content to the IT security company three times in 2023. Plaintiff's proposed injunction could be understood to prevent CISA from engaging with technology companies in this way or providing this service, thereby leaving the public at greater risk of being defrauded or compromised by these malicious sites, including those that impersonate the federal government itself.

29. In addition, Plaintiffs' proposed injunction could be understood to preclude CISA from "acting in concert" with "any such others who are engaged in the aforementioned conduct." This provision of the proposed injunction could be understood to mean that even if CISA is unaware that another entity is "engaged in the aforementioned conduct," CISA cannot "act[] in concert" with that entity for any purpose, even if CISA's interaction with the entity has nothing to do with a social media company's content moderation, including cyber threat removal, policies. In addition, it is unclear whether this provision of the proposed injunction means that CISA cannot "act[] in concert" with technology companies, including social media, if they themselves moderate content on their own platforms. If the proposed injunction were to be interpreted as prohibiting such interaction, CISA would be severely hindered in effectuating its statutory mission. Moreover, CISA would be placed in the impractical position of needing to inquire whether any partners engage in any of the expansively defined "aforementioned conduct" before engaging with them. If the Court were to impose such a broad injunction against CISA, CISA has identified the following additional examples of significant harm that could result to the agency, and it could be

left unable to fulfill its mission as operational lead for federal cybersecurity and the National Coordinator for critical infrastructure security and resilience:

a. Because Microsoft moderates content on some of its platforms or has publicly encouraged social-media companies to combat COVID-19 related misinformation, CISA could be unable to engage with Microsoft on cybersecurity or any other matter under this broad reading of Plaintiffs' proposed injunction.⁴ Microsoft is a multinational technology corporation for products and services such as Windows operating systems, the Microsoft Office suite, internet browsers Internet Explorer and Edge, cloud computing platform Azure, Active Directory, Xbox, and LinkedIn. CISA has daily engagement with Microsoft, which is necessary to fulfill the Agency's mission given the prevalence of Microsoft operating systems and software within FCEB and private sector networks. The inability to engage with Microsoft during a cyber incident could be catastrophic. For example, CISA's engagement with Microsoft was critical to securing the FCEB networks and critical infrastructure following the Russian Federation's supply chain compromise of SolarWinds Orion software in 2020, which impacted numerous federal and non-federal entities, and the People's Republic of China's mass exploitation of U.S.-based on-premise Microsoft Exchange mailservers in 2021. Under a broad reading of Plaintiffs' proposed injunction, CISA would not be able to work with this partner in the regular course or when similar cyber incidents occur in the future without running the risk that it could be accused of violating the injunction because Microsoft moderates content, including

⁴ See Meta, Working with Industry Partners (Mar. 16, 2020), <https://about.fb.com/news/2020/12/coronavirus/#joint-statement> (Joint industry statement from Facebook, Google, LinkedIn, Microsoft, Reddit, Twitter, and YouTube: "We are working closely together on COVID-19 response efforts. We're helping millions of people stay connected while also jointly combating fraud and misinformation about the virus, elevating authoritative content on our platforms, and sharing critical updates in coordination with government healthcare agencies around the world. We invite other companies to join us as we work to keep our communities healthy and safe.") (last visited April 24, 2023).

removing cyber threats, on some of its platforms and CISA could be regarded as “acting in concert” with it.

b. Because Google moderates content on some of its platforms or has publicly encouraged social-media companies to combat COVID-19 related misinformation, *see supra* note 4, CISA would be unable to engage with Google on cybersecurity or any other matter under this broad reading of Plaintiffs’ proposed injunction. Google is a multinational technology company providing, among other things, search engine technology, cloud computing, computer software, quantum computing, artificial intelligence, and YouTube. Through CISA’s JCDC, CISA regularly engages with Google and other members through this public-private partnership to proactively gather, analyze, and share actionable cyber risk information to enable synchronized, holistic cybersecurity planning, cyber defense, and response. *See* <https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative> (last visited April 24, 2023). Such engagement with Google could be prohibited under a broad interpretation of Plaintiffs’ proposed injunction because Google moderates content, including removing cyber threats, on some of its platforms and CISA could be regarded as “acting in concert” with it.

c. CISA may be unable to engage with the Center for Internet Security (CIS), the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) on cybersecurity, election security, and other matters, under this broad understanding of the proposed injunction, should CIS, or the MS- or EI-ISACs engage in any of the “aforementioned conduct.” CIS is a nonprofit organization that is home to the MS-ISAC and EI-ISAC. <https://www.cisecurity.org/about-us> (last visited April 24, 2023). The MS-ISAC serves as

a central cybersecurity resource for SLTT government entities, and the EI-ISAC supports the cyber and critical infrastructure security needs of U.S. elections offices and offers cyber defense tools. <https://www.cisa.gov/resources-tools/services/multi-state-information-sharing-and-analysis-center> (last visited April 24, 2023); <https://www.cisa.gov/resources-tools/groups/join-ei-isac> (last visited April 24, 2023). DHS has provided financial assistance to CIS through a series of cooperative agreement award, managed by CISA, to provide certain, specified cybersecurity services, such as cyber threat intelligence products, incident response and forensics, threat and vulnerability monitoring, cybersecurity awareness, and training products, to SLTT government organizations, which CIS accomplishes through the MS- and EI-ISACs. *See* Defs. Ex. 98 (CISA Hale Decl. ¶¶ 44-51). Yet under a broad reading of Plaintiffs’ proposed injunction, if CIS or the MS- or EI-ISACs were to flag disinformation for social media companies or engage in any other “aforementioned conduct,” even without CISA’s funding, involvement or knowledge, CISA might not be able to collaborate with them on any issue.

d. Should any of the Agency’s election security partners—such as state and local election officials (who are critical infrastructure owners and operators), the National Association of Secretaries of State, the National Association of State Election Directors, and the Election Infrastructure Subsector Coordinating Council and Government Coordinating Council—engage in any of the “aforementioned conduct,” plaintiffs might argue that the injunction prohibits CISA from separately engaging with these partners to secure the physical and cyber security of the systems and assets that support the nation’s elections. CISA engages with these election partners to provide physical and cybersecurity services and assessments, host exercises, and provide other support. *See*

<https://www.cisa.gov/topics/election-security> (last visited April 24, 2023); *see generally* Defs. Ex. 98 (CISA Hale Decl.). Again, under a broad reading of Plaintiffs’ proposed injunction, if any of these election security partners were to flag disinformation for social media companies or engage any of the other “aforementioned conduct,” even without CISA’s involvement or knowledge, CISA might not be able to collaborate with them on unrelated issues.

e. CISA might be unable to appoint representatives of technology companies who moderate content on their platforms, or representatives of state and local governments or other institutions should they engage in any of the “aforementioned conduct” to serve as members on the statutorily directed CSAC without running afoul of a broad understanding of Plaintiffs’ proposed injunction because CISA could be regarded as “acting in concert” with entities engaged in the prohibited “aforementioned conduct.” Consequently, plaintiffs might argue that the Agency would be precluded from receiving the advice and recommendations of, and consulting with some of the nation’s leading experts on cybersecurity.

30. These are just a handful of the serious potential impacts to CISA’s ability to secure and defend the nation’s cyberspace and critical infrastructure.

IV. Conclusion

31. If the proposed injunction is ordered, it could be understood in a manner that would prevent CISA from fulfilling its statutory mandate of securing and defending the nation’s cyber and critical infrastructure.

32. As a result, the proliferation of cyber and critical infrastructure threats affecting the American people could intensify, negatively impacting national security, national economic security, and national public health and safety.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge and belief. Executed on this 28 day of April, 2023.

**BRANDON D
WALES**

 Digitally signed by BRANDON D
WALES
Date: 2023.04.28 19:40:57 -04'00'

Brandon Wales
Executive Director
Cybersecurity and Infrastructure Security Agency

DEFENDANTS' EXHIBIT 168:

INTENTIONALLY LEFT BLANK

DEFENDANTS' EXHIBIT 169:

Hearing - Hearing Transcripts

Title Info

Title:	House Energy and Commerce Subcommittees on Communications and Technology and Consumer Protection Hold Joint Hearing on Misinformation and Disinformation on Online Platforms
Date:	March 25, 2021
Committee:	Energy and Commerce;HouseSubcommittee on Consumer Protection and Commerce. Committee on Energy and Commerce. House;Energy and Commerce;HouseSubcommittee on Communications and Technology. Committee on Energy and Commerce. House
Source:	Transcript
Permalink:	https://congressional.proquest.com/congressional/docview/t39.d40.tr03250121.h11?accountid=14740

Body

House Energy And Commerce Subcommittees On Communications And Technology And Consumer Protection Hold Joint Hearing On Misinformation And Disinformation On Online Platforms

March 25, 2021 12:00 P.M.

SPEAKERS:

REP. MICHAEL C. BURGESS (R-TEXAS)

REP DAVID B MCKINLEY (R W VA)

REP. LISA BLUNT ROCHESTER (D-DEL.)

REP. MORGAN GRIFFITH (R-VA.)

REP. KIM SCHRIER (D-WASH.)

REP DANIEL CRENSHAW (R TEXAS)

REP. JOHN JOYCE (R-PA.) HOUSE COMMITTEE ON ENERGY AND COMMERCE SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

REP. MIKE DOYLE (D-PA.), CHAIRMAN

REP. JERRY MCNERNEY (D-CALIF.)

REP. YVETTE D. CLARKE (D-N.Y.)

REP MARC VEASEY (D TEXAS)

REP. A. DONALD MCEACHIN (D-VA.)

REP. DARREN SOTO (D-FLA.)

REP. TOM O'HALLERAN (D-ARIZ.)

REP KATHLEEN RICE (D N Y)

REP. ANNA G. ESHOO (D-CALIF.)

REP G K BUTTERFIELD (D N C)

REP. DORIS MATSUI (D-CALIF.)

REP. PETER WELCH (D-VT.)

REP. KURT SCHRADER (D-ORE.)

REP TONY CARDENAS (D CALIF)

REP. ROBIN KELLY (D-ILL.)

REP. ANGIE CRAIG (D-MINN.)

REP. LIZZIE FLETCHER (D-TEXAS)

REP FRANK PALLONE JR (D N J), EX OFFICIO

REP. BOB LATTA (R-OHIO), RANKING MEMBER

REP. STEVE SCALISE (R-LA.)

REP. BRETT GUTHRIE (R-KY.)

REP ADAM KINZINGER (R ILL)

REP. GUS BILIRAKIS (R-FLA.)

REP. BILL JOHNSON (R-OHIO)

REP. BILLY LONG (R-MO.)

REP RICHARD HUDSON (R N C)

REP. MARKWAYNE MULLIN (R-OKLA.)

REP. TIM WALBERG (R-MICH.)

REP. EARL L. "BUDDY" CARTER (R-GA.)

REP JEFF DUNCAN (R S C)

REP. JOHN CURTIS (R-UTAH)

REP. CATHY MCMORRIS RODGERS (R-WASH.), EX-OFFICIO HOUSE COMMITTEE ON ENERGY AND COMMERCE
SUBCOMMITTEE ON CONSUMER PROTECTION

REP. JAN SCHAKOWSKY (D-ILL.), CHAIRWOMAN

REP. BOBBY L. RUSH (D-ILL.)

REP KATHY CASTOR (D FLA)

REP. LORI TRAHAN (D-MASS.)

REP. JERRY MCNERNEY (D-CALIF.)

REP. YVETTE D. CLARKE (D-N.Y.)

REP TONY CARDENAS (D CALIF)

REP. DEBBIE DINGELL (D-MICH.)

REP. ROBIN KELLY (D-ILL.)

REP. DARREN SOTO (D-FLA.)

REP KATHLEEN RICE (D N Y)

REP. ANGIE CRAIG (D-MINN.)

REP. LIZZIE FLETCHER (D-TEXAS)

REP FRANK PALLONE JR (D N J), EX OFFICIO

REP. GUS BILIRAKIS (R-FLA.), RANKING MEMBER

REP. FRED UPTON (R-MICH.)

REP. BOB LATTA (R-OHIO)

REP BRETT GUTHRIE (R KY)

REP. LARRY BUCSHON (R-IND.)

REP. NEAL DUNN (R-FLA.)

REP. GREG PENCE (R-IND.)

REP DEBBIE LESKO (R ARIZ)

REP. KELLY ARMSTRONG (R-N.D.)

REP. CATHY MCMORRIS RODGERS (R-WASH.), EX-OFFICIO

[*]DOYLE: The Subcommittee on Communications and Technology and Subcommittee on Consumer Protection and Commerce will now come to order. Today, we will be holding a joint hearing entitled Disinformation Nation: Social Media's Role in Promoting Extremism and Misinformation.

Due to the COVID-19 public health emergency, today's hearing is being held remotely. All members and witnesses will be participating via video conferencing. As part of our hearing, microphones will be set on mute for the purpose of eliminating inadvertent background noise

Members and witnesses, you will need to unmute your microphones each time you wish to speak. Additionally, members will need to be visible on screen in order to be recognized

Due to the anticipated length of this hearing, the committee will take a 15-minute recess around 3:00 to provide witnesses and members and restroom break Finally, documents for the record can be sent to Ed Hasmarski and Joe Orlando at the email addresses we have provided to your staff. All documents will be entered into the record at the conclusion of the hearing.

The chair will now recognize himself for five minutes.

Our nation is drowning in disinformation, driven by social media Platforms that were once used to share photos of kids with grandparents are all too often havens of hate, harassment, and division.

The way I see it, there are two faces to each of your platforms Facebook has Family and Friends Neighborhood, but it is right next to the one where there is a white nationalist rally every day. YouTube is a place where people share quirky videos, but down the street, anti-vaxers, COVID-deniers, QAnon supporters, and flat earthers are sharing videos. Twitter allows you to bring friends and celebrities into your home, but also holocaust deniers, terrorists, and worse

Now, it would be one thing if every user chose where to go organically, but almost everything is scripted on social media platforms Facebook recognizes anti social tendencies in one user and invites them to visit the white nationalists. YouTube sees another user as interested in COVID-19 and auto-starts an anti-vax video. On Twitter, a user following the trending conversation, never knowing it is driven by bots and coordinated disinformation networks, run by foreign agents.

Your platforms have changed how people across the planet communicate, connect, learn, and stay informed. The power of this technology is awesome and terrifying and each of you has failed to protect your users and the world from the worst consequence of your creations

This is the first time the three of you have appeared before Congress since the deadly attack on the Capitol on January 6th That event was not just an attack on our democracy and our electoral process, but an attack on every member of this committee and in the Congress.

Many of us were on the House floor and in the Capitol when that attack occurred and we were forced to stop our work of certifying the election and retreat to safety, some of us wearing gas masks and fearing for our lives. We fled as a mob desecrated the Capitol, the House floor, and our democratic process.

People died that day and hundreds were seriously injured. That attack and the movement that motivated it started and was nourished on your platforms. Your platforms suggested groups for people to join, videos they should view, and posts they should like, driving this movement forward with terrifying speed and efficiency.

FBI documents show that many of these individuals used your platforms to plan, recruit, and execute this attack. According to independent research, users on Facebook were exposed 1.1 billion times to misinformation related to the election last year alone, despite changes to your policies and claims that you've removed election misinformation.

Our nation is in the middle of a terrible pandemic. Nearly 550,000 Americans have lost their lives to this deadly disease, more than any other country on the planet. And an independent study found that on Facebook alone, that users across five countries, including the United States, were exposed to COVID disinformation an estimated 3.8 billion times, again, despite claims of fixes and reforms.

And now, as the Biden administration is working to implement the American Rescue Plan and get vaccines in people's arms, we are faced with waves of disinformation on social media about the safety and efficacy of these shots. These vaccines are our best chance we have to fight this virus and the content that your websites are still promoting, still recommending, and still sharing is one of the biggest reasons people are refusing the vaccine.

And, things haven't changed. My staff found content on YouTube telling people not to get vaccines and was recommended to similar videos. The same was true on Instagram, where it was not only easy to find vaccine disinformation, but platforms recommended similar posts. The same thing happened on Facebook, except they also had anti-vax groups to suggest as well. And Twitter was no different. If you go to any of these super-spreader accounts that remain up, despite the policies meant to curb this anti-vax content, you'll see this content.

Now, understand this. You can take this content down. You can reduce division. You can fix this. But, you choose not to.

We saw your platforms remove ISIS terrorist content. We saw you tamp down on COVID misinformation at the beginning of the pandemic. And, we have seen disinformation drop when you have promoted reliable news sources and remove serial disinformation super-spreaders from your platform.

You have the means, but time after time, you are picking engagement and profit over the health and safety of your users, our nation, and our democracy. These are serious issues and to be honest, it seems like you all just shrug off billion dollar fines. Your companies need to be held accountable. We need rules, regulations, technical experts in government, and audit authority of your technologies.

Our is the committee of jurisdiction and we will legislate to stop this. The stakes are simply too high.

The chair will now recognize Mr. Latta, ranking member of the Subcommittee on Communications and Technology, for five minutes for his opening statement.

LATTA: Well, I thank the chairman for recognizing me and I want to thank our witnesses for being with us today for a conversation that's long overdue in the Energy and Commerce Committee.

I'm deeply concerned by your decisions to operate your companies in a vague and bias manner with little to no accountability while using Section 230 as a shield for your actions and their real world consequences. Your companies have the power to silence the president of the United States, shut off legitimate journalism in Australia, shut down legitimate scientific debate on a variety of issues, dictate which articles or websites are seen by Americans when they search the internet. When these actions are taken, you just have little to no recourse to appeal the decision if they are aware of your actions. In most cases, we simply don't know.

What does this mean for everyday Americans? We are all aware of Big Tech's ever increasing censorship of conservative voices and their commitment to serve the radical progressive agenda by influencing a generation of children and removing shutting down or cancelling any news, books, and even now toys that aren't considered woke.

This is fundamentally un-American. At a recent hearing on disinformation and extremism online, Professor Turley, one of the nation's foremost experts on constitutional law, testified about the little brother problem, a problem which private entities do for the government which it cannot legally do for itself.

As of January of this year, Google has a greater than 92 market share and search. Facebook has over 2.7 billion--billion monthly users and Twitter has 187 million daily users. Your companies have enormous control over whose ideas are seen, read, or heard around the world. This gives you great power and if misused, as we have seen in recent years, your actions have a ripple effect throughout the world that result in American voices being removed from the marketplace of ideas.

While the little brother problem of censorship is frightening enough, other serious harms are occurring on these platforms that affect ordinary Americans. Young American children and teenagers are addicted--actually addicted--to their devices and social media. This problem has been exacerbated by the pandemic and will only get worse if children continue to be separated from their peers and cannot learn from their teachers in a classroom.

Your platforms are purposefully designed to keep our children hooked to their screens.

[*]LATTA: The use of social media has been linked to increased rates of depression, mental illness, cyber bullying, and suicide among America's youth. Illegal drugs continue to be sold online despite your previous commitments to sell these issues. Mr. Chairman, I a--I do ask unanimous consent to submit a letter to the National Association of Board of Pharmacy for the record.

DOYLE: Without objection, so ordered.

LATTA: Thank you very much. Serious problems continue to persist and I wonder how much you are truly dedicating to combating these actions. What actions are you taking to educate Americans about the dangers of using your site, especially the dangers for kids? As ranking member of the subcommittee on communications and technology, we have oversight of any change made to Section 230 of the Communications Decency Act.

Section 230 provides you with the--with liability protection for content moderation decisions made in good faith. Based on recent actions, however, it is clear that your definition of good faith moderation include censoring viewpoints you disagree with and establishing though independent appeals process that does not make its content moderation decision based on American principles of free expression. I find that highly concerning.

I look forward to today's hearing as an important step in reconsidering the extent to which big tech deserves to retain the significant liability protection. And with that, Mr. Chairman, I yield back the balance of my time.

DOYLE: Thank you. The gentleman yields back. The Chair now recognizes Chair Schakowsky, chair of the Subcommittee on Consumer Protection and Commerce, for five minutes for her opening statement.

SCHAKOWSKY: Thank you. It's a pleasure to cochair this meeting with you. I want to welcome our witnesses and thank them for coming. It is not an exaggeration to say that your companies have fundamentally and permanently transformed our very culture and our understanding of the world. Much of this is for good, but it is also true that our country, our democracy, even our understanding of what is truth has been harmed by the pro--the pro--proliferation and disse--and dissemination of this information and extremism, all of which is deeply divided us.

What our witnesses today need to take away from this hearing is that self-regulation has come to the end of its road. And that this democracy, this--this Democratic democ--the people that you see before you, elected by the people, is preparing to move forth with--with legislation and regulation. The regulation that we see should not attempt to limit constitutionally protected freedom of speech, but it must hold platforms accountable when they are used in--to incite violence and hatred or, as in the case of the COVID pandemic, spread misinformation that costs thousands of lives.

All three of the--of the companies that are here today run platforms that are hotbeds of misinformation and disinformation. And, despite all the promises and new policies to match, this disinformation was--this information was rampant in the 2020 election, especially targeting vuldermal--vulnerable communities. For example, Spanish-language ads run by the Trump adminis--the Trump campaign falsely accused President Biden of being endorsed by Venezuelan President Maduro.

The spread of disinformation fell--disinformation fed upon itself until it arrived at the Capitol of the United States on January 6th, which cost five lives. The lives lost in the insurgence--insurgency were not the first cases of these platforms' failure or more even the worst. In 2018, Facebook admitted a genocide of the Rohingya people in Myanmar was planned and executed on Facebook.

2020 saw the rise of a co--of coronavirus disinformation on Facebook platforms, including the playing of the--they called it the plandemic. This film got 1.8 million views and 150,000 shares before was removed. Disinformation like plan--plandemic made people skeptical of the need for vaccines and, almost certainly, cost--contributed to the

horrible loss of life during the pandemic.

Disinformation and also hops--hops platforms to spread viruses--I'm looking for a time. To--disinformation also hopes--hops from platform to--to platform--it be--plan--plandemic actually was first on YouTube before it was on Facebook and Instagram and Twitter.

Misinformation regarding the election dropped 73 percent across social media platforms after twitter permanently suspended Trump as well as on--on a--also--I'm sorry--okay--and also the capitol insurgency and QAnon.

But the question really is, what took so long? The witnesses here today have demonstrated time and time again that they--and--that--that they do not--that self-regulation has not worked. They must be held accountable for allowing disinformation and misinformation to--to spread. And that is why I--I'll be introducing the Online Consumer Protection Act which I hope will earn bipartisan support. And thank you, I yield back.

DOYLE: The gentlelady yields back. The chair now recognizes Mr. Bilirakis, Ranking Member for the subcommittee on consumer protection and commerce, for five minutes for his opening remarks.

BILIRAKIS: Thank you, Mr. Chairman. I appreciate it. Thank you for participating in today's hearing, all the witnesses and the members. I've been thinking about this hearing since our side first requested this hearing last year. My time in Congress has provided me enough knowledge about the history of the committee to know what the Telecommunications Act was and, importantly, what it wasn't.

Components of the--that law have been struck down by the courts while other provisions are interpreted and applied differently than first conceived. This is all a departure from congressional intent. Regardless of what one thinks or whether all of the Communications Decency Act was the right approach, the same members that voted for Section 230 voted for that entire bill. The statute was meant to protect our society, specifically her children.

To our witnesses today, here lies the problem for you. You don't want the federal government telling you what parts of your company you're allowed to operate. So, imagine things--imagine things from our perspective when you pick and choose what parts of the law you want to follow. I really do admire your ingenuity. You have created some--something truly remarkable in my opinion. But, with that power, you must also be good Samaritans. And you have an obligation to be stewards of your platform.

If your legal department doesn't believe you're bound to the intent of the law, I would hope your moral compasses will. Many of my colleagues will raise legitimate concerns about the attack on the Capitol from January. And other colleagues can point to what occurred in our cities last summer. These were all incidents where social media escalated tension, incited chaos, and bred extremism through echo chambers and algorithms.

As the new Republican leader--quite an honor--on the Commerce Protection and com--Commerce Committee--so the Consumer Protection Commerce Committee, I have been digging into how your companies operate. That led me to run a survey--survey of my district following our big tech hearing announcement.

[*]BILIRAKIS: The conclusion is my constituents simply don't trust you anymore. With thousands of responses over 82 percent say they do not trust big tech to be good stewards of their platform or consistently enforce their policies. That includes my constituent who told me, we were providing information to local families on teen suicide risks on Facebook livestream. It was blocked by Facebook.

Another constituent she has seen countless teens be bullies online or simply not able to process a devastating comparison game that they are forced to deal with on social media. Others told me they stopped using your services all together out of fear and distrust.

One even told me they quit social media due to treatment by your companies over their family's Christian views. Each one of these represents a story of how your companies have failed people. And you'll be hearing from my colleagues with more of these stories about how big tech has lost its way highlighting a much larger problem.

People want to use your services but they suspect your coders are designing what they think we should see and hear by keeping us online longer than ever and all with the purpose to polarize or monetize us. Disregarding any consequences for that assault--for an assault on our inherent freedoms, which we hold so dearly.

So I don't want to hear about how changing your current law is going to--for startups because I heard directly from them accusing you of anticompetitive factors. None of us want to damage entrepreneurs. What I do want to hear is what you will do bring our country back from the fringes and stop the poisonous practices that drive

depression, isolation and suicide. And instead, cooperate with law enforcement to protect our citizens.

Our kids are being lost while you say you will try to do better as we have heard countless times already. We need true transparency and real change. We need again, not empty promises from you. We have heard that over and over again.

The fear you should have coming into this hearing today isn't that you are going to get upgraded (PH) by a member of Congress—it's that our committee knows how to get things done when we come together. We can do this with you or without you and we will. Thank you, Mr. Chairman. I yield back.

DOYLE: Gentleman yields back. Chair now recognizes Mr. Pallone, chairman of the Full Committee, for five minutes for his opening statement.

PALLONE: Thank you, Chairman Doyle and Schakowsky for this very important hearing. We're here today because the spread of disinformation and extremism has been growing online particularly, in social media where there are little to no guard rails in place to stop it. And unfortunately, this disinformation and extremism doesn't just stay online it has real world, often dangerous and even violent consequences and the time has come to hold online platforms accountable for their part in the rise of disinformation and extremism.

According to a survey conducted by (INAUDIBLE) earlier this month, 30 percent of Americans are still hesitant or simply do not want to take the COVID-19 vaccine. On January 6th, our nation's capital was violently attacked—this month Homeland Security Secretary Mayorkas identified domestic violent extremism as the greatest threat to the United States. In crimes against Asian Americans have risen by nearly 150 percent since the beginning of the COVID-19 pandemic.

Each of these controversies and crimes have been accelerated and amplified on social media platforms through misinformation campaigns, the spread of hate speech and the proliferation of conspiracy theories.

Five years ago during the 2016 presidential elections, Facebook, Google and Twitter were warned about but simply ignored their platform's role in spread disinformation. And since then, the warnings have continued but the problem has only gotten worse. Only after public outrage and pressure did these companies make inadequate attempts to appease critics and lawmakers. But despite the public rebuke, Wall Street continued to reward the company strategies to promote misinformation and disinformation by driving their stock prices even higher.

And now, despite repeated promises to seriously tackle this crisis, Facebook, Google and Twitter instead routinely make minor changes to their policies in response to the public relations crisis of the day and they will change some underlying internal policy that may or may not be related to the problem but that's it.

The underlying problem remains. So Mr.—Mr. Chairman it is now painfully clear that neither the market nor public pressure will force these social media companies to take the aggressive action they need to take to eliminate disinformation and extremism from their platforms.

And therefore, it's time for Congress and this committee to legislate and realign these companies incentives. Today, our laws give these companies and their leaders a blank check to do nothing rather than limit the spread of disinformation, Facebook, Google and Twitter have created business models that exploit the human's brain preference for divisive content to get Americans hooked on their platforms at the expense of the public interest.

And it isn't just that social media companies are allowing disinformation to spread it is that in many cases they are actively amplifying and spreading it themselves. And fines, to the extent they are levied at all have simply become the cost of doing business.

The dirty truth, is that they are relying on algorithms to purposely promote conspiratorial, divisive or extremist content so that they can take money—more money and add dollars. And this is because the more outrageous and extremist the content the more engagement and views these companies get from their users and more views equals more money, Mr. Chairman. That's what it's all about—more money.

It's crucial to understand that these companies are just mere bystanders they are playing an active role in the meteoric rise of disinformation and extremism because they make money on it. So when a company is actually promoting this harmful content, I question whether existing liability protections should apply.

Members on this committee have suggested legislative solutions and introduced bills. The committee is going to consider all these options so that we can finally align the interests of these companies with the interests of the public and hold the platforms and their CEOs accountable when they strike.

That's why you're here today Mr. Zuckerberg, Mr. Pichai and Mr. Dorsey--you have failed to meaningfully change after your platforms played a role in fermenting insurrection, in a bedding the spread of the virus and trampling American civil liberties.

And while it may be true that some bad actors will shout fire in a crowded theater by promoting harmful content your platforms are handing them a megaphone to be heard in every theater across the country and the world.

Your business model itself has become the problem and the time for self-regulation is over. It's time to legislate to hold you accountable. That's what we're going to do and I want to thank you, Mr. Chairman, Mr. Doyle and Ms. Schakowsky, because know that you're very serious about moving forward on legislation which we will do, I promise everyone. Thank you and I yield back.

DOYLE: Gentleman yields back. The chair now recognizes Ms. Rodgers, the ranking members of the full committee for five minutes for her opening statement.

RODGERS: Thank you, Mr. Chairman. Ten years ago, when I joined big tech platforms I thought it would be a force for good. I thought they would help us build relationships and promote transparency in Congress. I can testify today, I was wrong. That is not what has transpired. You have broken my trust.

Yes, because you failed to promote the battle of ideas and free speech. Yes, because you censored political viewpoints you disagree with. Those polarizing actions matter for democracy.

But do you know what convinced me big tech is a--is a destructive force? It's how you've abused your power to manipulate and harm our children. Your platforms are my biggest fear as a parent. I'm a mom of three school age kids and my husband and I are fighting the big tech battles in our household every day. It's a battle for their development, a battle for their mental health and ultimately, a battle for their safety. I've monitored your algorithms. I've monitored where your algorithms lead them. It's frightening.

And I know that I am not alone. After multiple teenage suicides in my community, I've reached out to our schools and we started asking questions--what's going on with our kids? What's making them feel so alone, so empty and in despair? And this is what I heard over and over again from parents, pediatricians, school administrators and teachers--they're all raising the alarm about social media.

A day doesn't go by that I don't talk to friends and other parents who tell me their 14-year-old is depressed. She used to love soccer. Now they can't get her to do anything. She never gets off her device or leaves her room.

I--I think about a mom who told me she can't leave her daughter alone ever because she harms herself or the family who's recovering, after almost losing their daughter to a predator she met online. These stories are not unique to me or Eastern Washington.

I recently heard of a young college student who has lost nine friends to suicide. This is unimaginable. The science on social media is becoming clear. Between 2011 and 2018, rates of depression, self-harm, suicides, and suicide attempts exploded among American teens.

During that time, rates of teen depression increased more than 60 percent with a larger increase among young girls. Between 2009 and '15, emergency room admissions for self-harm among 10 to 14 year old tripled and suicide substantially increased.

One study found during that time, teens who used their devices for five or more hours a day were 66 percent more likely to have at least one suicide related outcome compared to those who used their device for just one. Other studies found that teens who spend more time online report lower psychological wellbeing and more feelings of loneliness.

Remember, our kids, the users, are the product. You, big tech, are not advocates for children. You exploit and profit off of them. big tech needs to be exposed and completely transparent for what you are doing to our children so parents like me can make informed decisions.

We also expect big tech to do more to protect children because you haven't done enough. big tech has failed to be good stewards of your platforms.

I have--I have two daughters and a son with a disability. Let me be clear. I do not want you defining what is true for them. I do not want their future manipulated by your algorithms. I do not want their self-worth defined by the engagement tools you built to attract their attention. I do not want them to be in danger from what you've created.

I do not want their emotions and vulnerabilities taken advantage of, so you can make more money and have more power.

I'm sure most of my colleagues on this committee, who are parents and grandparents, feel the same way. Over 20 years ago, before we knew what big tech would become, Congress gave you liability protections.

I want to know, why do you think you still deserve those protections today? What will it take for your business model to stop harming children?

I know I speak for millions of moms when I say we need answers and we will not rest until we get them. Thank you.

DOYLE: Thank the gentlelady. Gentlelady yields back. The chair would now like to remind members that pursuant to committee rules, all members' written opening statements shall be made a part of the record.

I would now like to introduce our witnesses for today's hearing and thank them all for appearing today. First, we have Mark Zuckerberg, chairman and chief executive officer of Facebook, Sundar Pichai, chief executive officer of Google, and Jack Dorsey, chief executive officer of Twitter.

We want to thank all three of you for joining us today. We look forward to your testimony. Each of you will have five minutes to give your opening statements. Mr. Zuckerberg, we'll start with you. You're recognized for five minutes.

ZUCKERBERG: Chairs Pallone and Schakowsky and Doyle, Ranking Members Rodgers, Latta, and Bilirakis, and members of the committee. I'm glad that this committee is looking at all of the ways that misinformation and disinformation show up in our country's discourse. There are important challenges here for our society and we have to decide how we want to handle speech that is legal but harmful and who should be responsible for what people say.

Misinformation is not a new problem. It was 200 years ago that a congressman said that a lie would travel from Maine to Georgia while truth was still getting on his boots, and disinformation has often been spread through traditional media too. But the internet gives everyone the power to communicate and that certainly presents unique challenges.

Now, people often say things that aren't verifiably true but that speak to their lived experiences, and I think we have to be careful restricting that. For example, if someone feels intimidated or discriminated against while voting, I believe that they should be able to share their experience, even if the election overall was fair.

I don't think anyone wants a world where you can only say things that private companies judge to be true, where every text message, email, video, and post has to be fact checked before you hit send. But, at the same time, we also don't want misinformation to spread that undermines confidence in vaccines, stops people from voting, or causes other harms.

At Facebook, we do a lot to fight misinformation. We remove content that could lead to imminent real-world harm. We've built an unprecedented third-party fact checking program and if something is rated false, then we add warning labels and significantly reduce its distribution. We invest a lot in directing billions of people to authoritative information.

This system isn't perfect, but it's the best approach that we've found to address misinformation in line with our country's values. It's not possible to catch every piece of harmful content without infringing on people's freedoms in a way that I don't think that we'd be comfortable with as a society.

Our approach was tested in 2020 when we took extraordinary steps during an extraordinary election. We removed voting misinformation, banned hundreds of militias and conspiracy networks including QAnon, labeled posts that prematurely or wrongly declared victory, and directed people to official results.

We labeled over 180 million posts, we directed 140 million people to our official Voting Information Center and we helped 4 and a half million people register to vote. We did our part to secure the integrity of the election and then on January 6th, President Trump gave a speech rejecting the results and calling on people to fight.

The attack on the Capitol was an outrage and I want to express my sympathy to all of the members, staff, and Capitol workers who had to live through this disgraceful moment in our history. And I want to express my gratitude to the Capitol Police who were on the frontlines in defense of our democracy.

Now, I believe that the former president should be responsible for his words and that the people who broke the law should be responsible for their actions. So, that leaves the question of the broader information ecosystem and I can't speak for everyone else, the TV channels, radio stations, news outlets, websites, and other apps, but I can tell you what we did.

Before January 6th, we worked with law enforcement to identify and address threats. During and after the attack, we provided extensive support in identifying the insurrectionists and removed posts supporting violence. We didn't catch everything, but we made our services inhospitable to those who might do harm and when we feared that he would incite further violence, we suspended the former president's account.

Now, many people are concerned that platforms can ban elected leaders. I am too. I don't think that private companies should make so many decisions like this alone. We need an accountable process, which is why we created an Independent Oversight Board that can overrule our decisions and we need democratically agreed rules for the internet.

The reality is our country is deeply divided right now and that isn't something that tech companies alone can fix. Now, we all have a part to play in helping to turn things around and I think that starts with taking a hard look at how we got here.

Now, some people say that the problem is that social networks are polarizing us, but that's not at all clear from the evidence or research. Polarization was rising in America long before social networks were even invented and it's falling or stable in many other countries where social networks are popular.

Others claim that algorithms feed us content that makes us angry because it's good for business, but that's not accurate either. I believe that the division we see today is primarily the result of a political and media environment that drives Americans apart, and we need to reckon with that if we're going to make progress.

Now, I know that technology can help bring people together. We see it every day on our platforms. Facebook is successful because people have a deep desire to connect and share, not to stand apart and fight, and we believe that connectivity and togetherness are more powerful ideals than division and discord and that technology can be part of the solution to the challenges our society is facing, and we are ready to work with you to move beyond hearings and get started on real reform. Thank you.

[*]DOYLE: Thank you, Mr. Zuckerberg. Now, Mr. Pichai, you are now recognized for five minutes.

Mr. Pichai, are you unmuted?

PICHAH: I didn't have my volume on.

Chairman Doyle, Ranking Member Latta, Chairman–Chairwoman Schakowsky, Ranking Member Bilirakis, Full Committee Chair Full Committee Ranking Member Pallone, and Ranking Member McMorris Rodgers, and members of the committee, thank you for the opportunity to appear before you today.

To begin, I want to express my sympathies to those who have lost loved ones to COVID or the recent gun violence in Boulder and Atlanta. In difficult times, we're reminded of what connects us as Americans, the hope that we can make things better for our families and our communities. And we, at Google, are committed to that work.

I joined Google because I believe to the Internet was the best way to bring the benefits of technology to more people. For the past three decades, we have seen how it's inspired the best in society by expanding knowledge, powering businesses, and providing opportunities for discovery and connection. I'm proud that anyone can come to Google for help, whether they are looking for vaccine information, learning new skills on YouTube, or using digital tools to grow their businesses.

In 2020, our products helped 2 million U.S. businesses and publishers generate \$426 billion in economic activity. We are energized by the opportunity to help people that scale, and humbled by the responsibility that comes with that. Thousands of people at Google are focused on everything from cyber attacks to privacy to today's topic, misinformation. Our mission is to organize the world's information and make it universally accessible and usable.

Core to that is providing trustworthy content and opportunities for free expression while combating misinformation. It's a big challenge without easy answers. Five-hundred plus hours of video are uploaded to YouTube every minute, and approximately 15 percent of Google searches each day are new to us. 18 months ago, no one had heard of COVID-19. Sadly, coronavirus was the top trending search last year.

Staying ahead of new challenges to keep users safe is a top priority. We saw the importance of that on January 6th when a mob stormed the U.S. Capitol. Google strongly condemns these violent attacks on our democracy and mourns the lives lost. In response, we raised up authoritative sources across our products. On YouTube, we removed live streams and videos that violated our incitement to violence policy and began issuing strikes to those in violation of our presidential elections' policy.

We removed apps from the play store for inciting violence and stopped ads referencing the 2020 election or the Capitol riots as part of our sensitive events policy. We were able to act quickly because we were prepared ahead of the 2020 elections. Our reminders of how to register and vote were viewed over 2 billion times. YouTube's election results information panels have been viewed more than 8 billion times.

We also worked to keep campaign safe from cyber attacks and protect platforms from abuse. After the December 8 Safe Harbor deadline for states to certify elections, we removed content from YouTube that alleged widespread fraud changed the outcome of the election. This past year, we've also focused on providing quality information during the pandemic. Globally, we have committed over \$550 million and add grants for COVID related PSAs to governments, health organizations, and nonprofits.

On YouTube, our COVID information panels have been viewed over 400 billion times. We also removed 850,000 videos and blocked nearly 100 million COVID related ads throughout 2020. Across all of this work, we strive to have transparent policies and enforce them without regard to politics or point of view.

Our ability to provide a range of information and viewpoints while also being able to remove misinformation is possible only because legal frameworks like Section 230. It's foundational to the open (INAUDIBLE) which has been a powerful force for good for so many. I look forward to sharing more about our approach today and working together to create a path forward for the web's next three decades. Thank you.

DOYLE: Thank you, Mr. Pichai. The chair now recognizes Mr. Dorsey for five minutes.

DORSEY: Thank you, members of the Energy and Commerce Committee and its subcommittees for the opportunity to speak with the American people about how Twitter may be used to spread disinformation and our solutions. My remarks will be brief so we can move to your questions and discussion.

In our discussion today, some of you might bring up specific tweets or examples, and I'll probably have an answer like, my team will follow up with you. I don't think that's useful. I'd rather us focus on principles and approaches to address these problems. I'll start with ours. We believe in free expression; we believe in free debate and conversation to find the truth.

At the same time, we must balance that with our desire to—for our service not to be used to sow confusion, division, or destruction. This makes the freedom to moderate content critical to us. Our process to moderate content is designed to constantly evolve. We observe what's happening on our service, we work to understand the ramifications, and we use that understanding to strengthen our operations.

We push ourselves to improve based on the best information we have. Much of what we're likely to discuss today are entirely new situations the world has never experienced before. And, in some unique cases, involve elected officials.

And we believe the best way to face a big new challenges through narrowing the problem to have the greatest impact. Disinformation is a broad concept. We need to focus our approach on where we saw the greatest risk if we hope to have any impact at all.

So, we chose to focus on disinformation leading to off-line harm, in three categories to start, manipulated media, public health, and civic integrity. Many of you will have strong opinions on how effective we are in this work. Some of you will say we're doing too much and removing free-speech rights. Some of you will say we're not doing enough and end up causing more harm. Both points of view are reasonable worth exploring.

If we woke up tomorrow and decided to stop moderating content, we did up with the service very few people or advertisers would want to use. Ultimately, we're running a business. And the business wants to grow the number of customers it serves. Enforcing policies is a business decision. Different businesses and services will have different policies. Some more liberal than others. And we believe it's critical this variety continues to exist. Forcing every business to behave the same reduces innovation and individual choice and diminishes free marketplace ideals.

If, instead, we woke up tomorrow and decided to ask the government to tell us what content to take down or leave up, we may end up with the service that couldn't be used to question the government. This is a reality in many countries today and is against the right of an individual. This would also have the effect of putting enormous resource requirements on businesses and services which would further entrench only those who are able to afford it. Small businesses would not be able to compete and all activity would be centralized into very few businesses.

So, how do we resolve these two viewpoints? One way is to create shared protocols. Social media has proven itself important enough to be worthy of an Internet protocol, one that a company like Twitter can contribute to and compete on creating experiences people love to use. We started work on such a protocol, which we call Bluesky. Intends to act as a decentralized, open source social media protocol, not owned by any single company or organization. Any developer around the world can help develop it just as any company can access and services.

How does an open protocol address the concerns raised here? Greater transparency is its strongest benefit. Anywhere--anyone around the world can see everything that's happening in the network including exactly how it works.

One doesn't have to trust a company, just look at the source code. Second, since the base protocol is shared, it will increase innovation around business models, recommendation algorithms, and moderation controls which are in the hands of individuals rather than private companies. This will allow people to experiment in a market-based approach.

Finally, it will allow all of us to observe, acknowledge, and address any societal issues that arise much faster. Having more eyes on the problems will lead to more impactful solutions that can be built directly into this protocol, making the network far more secure and resilient.

A decentralized open-source protocol for social media is our vision and work for the long-term. We continue the cycle mentioned earlier of constantly improving our approach to content moderation in the short term. I hope our discussion today will focus on more enduring solutions.

One final note, we are a bunch of humans with a desire to make the world around us better for everyone living today and those that come after us. We make mistakes and prioritization and in execution. We commit to being open about these and doing our best to remedy what we control. We appreciate the enormous privilege we have in building technologies to host some of the world's most important conversations.

[*]DORSEY: And we honor the desire to create better outcomes for everyone who interacts with them. Thanks for your time and I look forward to the discussion.

DOYLE: Thank you, Mr. Dorsey. While we've concluded witness opening statements at this time, we will move to member questions. I want to make sure that members are aware that our members are being assisted by counsel and during questions our witnesses may briefly mute themselves to seek advance--advice of counsel which is permitted.

Each member will have five minutes to start asking questions for our witnesses. I ask everyone to please adhere to that five minute rule as we have many people that want to ask questions. I will start by recognizing myself for five minutes.

DUNCAN: Chairman, point of order.

DOYLE: Gentleman who--who is speaking?

DUNCAN: Jack Duncan. Point of order.

DOYLE: Yes, sir.

DUNCAN: If the witness, if the witnesses are advised by counsel we're not swearing them in, why would they need counsel?

DOYLE: In--in previous hearings we've always permitted witnesses to have counsel. Sometimes you'll see them in a hearing just leaning back and talking to their counsel before question. But it's allowed under our rules and--and I just wanted to make members aware that they may mute themselves while that's going on.

DUNCAN: They should be sworn in. I yield back. Thank you.

DOYLE: Thank you. Ok. Gentleman, my time is short and I ask that you make your responses as brief and to the point as possible. If I ask you a yes or no question, I'm just looking for a yes or not so please respond appropriately. I want to start by asking all three of you if your platform bears some responsibility for disseminating disinformation related to the election and the stop the steal movement that led to the attack on the Capitol? Just a yes or no answer. Mr. Zuckerberg?

ZUCKERBERG: Chairman, I think our responsibility is to build systems that can help--

DOYLE: Mr. Zuckerberg, I just want a yes or no answer, Ok? Yes or no do you bear some responsibility for what happened?

ZUCKERBERG: Congressman, our responsibility is to make sure we build effective systems--

DOYLE: Okay the gentleman has decided not to answer the question. Mr. Pichai, yes or no?

PICHAJ: We always feel a deep sense of responsibility but I think we worked hard this election, in fact, it was one of our most substantive efforts.

DOYLE: Is that a yes or a no?

PICHAJ: Congressman, it's a complex question. We--

DOYLE: Okay. We'll move on. Mr. Dorsey?

DORSEY: Yes, but you also have to take into consideration a broader ecosystem. It's not just the technology platforms we use.

DOYLE: Thank you. Thank you and I agree with it. Mr. Zuckerberg, independent analysis has shown that despite all the things that Facebook did during the election, users still interacted with election misinformation roughly 1.1 billion times over the last year. The initial Stop the Steal group started on Facebook and gained over 350,000 followers in less than a day. Faster than almost any other in your platform's history. And they were immediately calling for violence.

In mid-December you stopped promoting high quality news outlets for election content at a time when the disinformation was at its height. And finally, the FBI has released numerous documents showing that many of the insurrectionists use Facebook to coordinate and plan the attack on January 6th. So my question is--how is it possible for you not to at least admit that Facebook played a central role or--or a leading role in facilitating the recruitment, planning and execution of the attack on the Capitol?

ZUCKERBERG: Chairman, my--my point is that I think that the responsibility here lies with the people who took the actions to break the law and take and do the insurrection. And secondarily, also the--the people who spread that content including the president but others as well with repeated rhetoric over time saying that the election as rigged and encouraging people to organize I think that those people bear the primary responsibility as well. And that was the point that I was making.

DOYLE: I understand that but your platforms super charged that. You--you took what a thing and magnified it 12 hours. You got 350,000 people in--in your site. You--you jiggled this up your algorithms make it possible to supercharge these kinds of opinions. I think we're here because of what these platforms enable, how your choices you know, put our lives and our democracy at risk. And many of us just find it just-just unacceptable. I want to ask each of you another question--do you think vaccines that have been approved for COVID-19 work? Just a yes or no. Do you think the vaccines that have been approved for it--Mr. Zuckerberg?

ZUCKERBERG: Yes.

DOYLE: Mr. Pichai?

PICHAJ: Yes. Absolutely.

DOYLE: Mr. Dorsey?

DORSEY: Yes. But I don't--I don't think we're here to discuss our own personal opinions--

DOYLE: I just want to know if you think the vaccines work, yes?

DORSEY: Yes. However (INAUDIBLE)--

DOYLE: Thank you. Ok. So if you think the vaccines work--why have your companies allowed accounts that repeatedly offend your vaccine disinformation policies to remain up? I mean, according to report just 12 accounts on Facebook, Twitter and Instagram account for 65% of all the vaccine disinformation on your platforms.

You're exposing 10s of millions of users to this every day. I--I don't have the stats on YouTube but my understanding is it's similar. So my--my question is--why in the midst of a global pandemic that has killed over half a million Americans that you haven't taken these accounts down that are responsible for the preponderance of vaccine disinformation on your platforms? Will you all commit to taking these platforms down, today? Mr. Zuckerberg?

ZUCKERBERG: Congressman, yes, we do have a policy against a--allowing vaccine misinformation--

DOYLE: I know you have a policy--but will you take the sites down today? You still have 12 people up on your site doing this--will you take them down?

ZUCKERBERG: Congressman, I would need to look at the--and--and have our team look at the exact examples to make sure they violate our policy. (INAUDIBLE) we have a policy in place for this.

DOYLE: Because those still exist. We found them as early as last night. Mr. Pichai, how about you?

PICHAJ: We have removed over 850,000 videos in--

DOYLE: Do you still have people that are spreading disinformation on your platforms? There's about 12 super spreaders.

PICHAJ: We have clear policies and we take down content. Some of the content is allowed if it's people personal experiences but you know, we--we definitely--

DOYLE: OK. Mr. Dorsey--I see my time is getting expired. Mr. Dorsey--will you take these sites down? You have about 12 super spreaders. Will you take them down?

DORSEY: Yes, we remove everything against our policy.

DOYLE: Thank you. I see my time has expired. I will now yield to the Ranking Member, Mr. Latta, for his five minutes.

LATTA: I thank my friend for yielding. Amanda Todd was just 15 years old when she hung herself. Amanda met a man--met a man online, who took inappropriate screenshots of Amanda and proceeded to follow her around the internet and harass her for years. He found her classmates on Facebook--he would send them the picture he took of her. To cope with the anxiety, Amanda turned to drugs and alcohol. It became too much for her.

Mr. Zuckerberg, clearly Ms. Todd was underage so the photo that was shared by her harasser was illegal. Do you believe that Facebook bears any responsibility for the role it played in her death--yes or no?

ZUCKERBERG: Sorry, I was muted. Congressman, that is a--it's a incredibly sad story and--I--I think that we certainly have a responsibility to make sure that we're building systems that can fight and remove this kind of harmful content. In the--in the case of child exploitation content we've been building systems for a long time that use AI and we have thousands of people working on being able to identify this content and remove it. And I think our systems are generally pretty effective at this. And I--and I think it's a responsibility to make sure (INAUDIBLE) we keep improving them.

LATTA: --My time is pretty short but would you say yes or no then?

ZUCKERBERG: Sorry. Can you repeat that?

LATTA: Well, in--in a question--yes or no then any responsibility?

ZUCKERBERG: Congressman, I believe that the responsibility of the platforms--

LATTA: Let me move on then. I'm very short on time. Do you believe that Facebook should be held accountable for any role in her death, yes or no?

ZUCKERBERG: Congressman, the responsibility that I think platforms should have is to build effective systems to moderate this content.

LATTA: (INAUDIBLE) just not responding to the question. Unfortunately, stories like Amanda Todd's are only becoming more common. What we often talk about how your platforms can be used for good and evil the evil seems to persevere. Mr. Zuckerberg, you publicly stated that you support thoughtful change to Section 230 to ensure that tech companies are held accountable for certain actions that happen on their platforms such as child exploitation. What specific changes do you support in Section 230?

ZUCKERBERG: Thanks, Congressman. I--I would support two specific changes, especially for large platforms. Although I--I want to call out that I think for--for smaller platforms I think we need to be careful about--about any changes that we make that remove their--their immunity, because that could hurt competition.

So, let me just call on these for larger platforms. I think first, platforms should have to issue transparency reports that--that state the prevalence of content across all different categories of harmful content, everything from child exploitation to terrorism to incitement of violence to intellectual property violations to pornography, whatever the different harms are and so--

LATTA: --Let me ask you quick now, where are those transparency reports being reported to and--and how often do you think those should be going out?

ZUCKERBERG: Well, Congressman, as--as a model, Facebook has been doing something to this effect for every quarter, right, where we report on the prevalence of each category of harmful content and how effective our systems are at identifying that content and removing it in advance, and--and I think the companies should be held accountable for having effective systems to do that broadly.

The second change that I would propose is--is--is creating accountability for the large platforms to have effective systems in place to moderate and remove clearly illegal content. So, things like sex trafficking or child exploitation or terrorist content, and I think it would be reasonable to condition immunity for the larger platforms on having a generally effective system in place to moderate clearly illegal types of content.

LATTA: --Let me interrupt real quick because I am running really short on time, because I know in your testimony, you're talking about that you would--you say that platforms should not be held liable if a particular piece of content evades this detection. So, again, that's one of the areas, when you're talking about the transparency and also the accountability, I'd like to follow up on.

Let me--I'm going to have to go on real quick. Mr. Pichai, yes or no, do you agree with Mr. Zuckerberg's changes to Section 230?

PICHAJ: There are definitely good proposals around transparency and accountability, which I've seen in various legislative proposals as well, which I think are important principles and--and we would certainly welcome legislative approaches in that area.

LATTA: Okay. Mr. Dorsey, do you agree with Mr. Zuckerberg, yes or no, on changes on 230?

DORSEY: I think the ideas around transparency are good. I think it's going to be very hard to determine what--what's a large platform and a small platform and it may incentivize the wrong things.

DOYLE: Okay, the gentleman's time has expired.

LATTA: Thank you very much. My time has expired, and I yield back.

DOYLE: Chair now recognizes Chair Schakowsky, Chair of the Subcommittee on Consumer Protection and Commerce, for five minutes.

SCHAKOWSKY: Thank you so much. Mr. Zuckerberg, immediately after the Capitol insurgency, Sheryl Sandberg did an interview in which she insisted that the siege was largely planned on smaller platforms that--but court filings actually show something quite the--quite the opposite, that the Proud Boys and Oath Keepers used Facebook to coordinate in real time during the--during the siege.

And, so my question for you is, will you admit today that Facebook groups in particular played a role in the--in fermenting the extremism that we saw and that led to the Capitol siege?

ZUCKERBERG: Congresswoman, thanks for the--the question on this. In--in the comment that--that Sheryl made, what--what I believe that we were trying to say was--and what I stand behind--is what was widely reported at the time, that after January 6th--

SCHAKOWSKY: --I'm sorry to interrupt, as many of my colleagues have had to do, because we only have five minutes. But, would you say that--and would you admit that Facebook played a role?

ZUCKERBERG: Congresswoman, I think certainly there was content on our services and--and from that perspective, I think that there's further work that we need to do to make our services and moderation more effective.

SCHAKOWSKY: --I hear that. I hear that. Okay, I'm going to ask Mr. Pichai a question. Many companies have used Section 230 as a shield to escape consumer protection laws and I have a bill that would actually not protect companies that--that do that and so Mr. Pichai, would you agree that that would be a proper use to not allow liability protection for those who violate consumer protection laws?

PICHAJ: Congresswoman, consumer production laws are very important in many areas, like--like we comply with COPPA and HIPAA. I think the right approach is to have legislation in applicable areas and have us--

SCHAKOWSKY: --Okay, I'm going to have to--I'm going to have to interrupt again. Is that a yes, that if a law has been broken, a consumer protection law, that it would not--there would not be liability protection under Section 230 for you?

PICHAJ: We rely on the liability protections to actually take strong action in particularly new types of content. When the Christchurch shooting happened, within a few minutes, our teams have to make decisions about the content to take down. That certainly is what we rely on. But, I agree with you that we should have strong consumer protection laws and be subject to it and have agencies like the FDC, have clear oversight over those laws and how we comply with them.

SCHAKOWSKY: Let me just ask a real yes or--thank you--a real yes or no quickly. Do you think that when you take money to run advertisements that promote disinformation, that you are exempt from liability? Yes or no? Yes or no?

PICHAJ: Yes, Section 230--

SCHAKOWSKY: --Mr. Zuckerberg, yes or no?

ZUCKERBERG: Congresswoman, I--I don't know the legal answer to that, but we don't allow misinformation in our ads and any ad that's been fact checked as false, we don't allow it to run as an ad.

SCHAKOWSKY: Okay, and Mr. Dorsey?

DORSEY: Again, I also would need to review the legal precedent for it, but we would--we would not allow that.

SCHAKOWSKY: Okay, and Mr. Pichai?

PICHAJ: We are subject to FDC's deceptive ad practices, so there's statutes which apply to us. We removed over 3 million bad ads last year alone.

SCHAKOWSKY: Okay, let me ask one more question. Do you think that Section 230 should be expanded to trade agreements that are being made, as happened in the U.S. trade agreement with Mexico and Canada? Yes or no? Mr. Zuckerberg?

ZUCKERBERG: Congresswoman, my primary goal would be to help update Section 230 to reflect the--the--the kind of modern reality and what we've learned over 25 years. With that said, I do still think that Section 230 plays a foundational role in the development of the internet and companies getting built. So--so, I do think that we should support it.

SCHAKOWSKY: --Okay, I hear you. I'm talking now about trade agreements. Mr. Pichai?

PICHAJ: Congresswoman, I think there's value in it, but if there are evolution of Section 230, that should apply and so, in a flexible way, being able to do that would be--would be good I think.

SCHAKOWSKY: Mr. Dorsey?

DORSEY: I don't fully understand the ramifications of what you're suggesting, so I'd have to review--

SCHAKOWSKY: --I said to have a liability shield that would be international and ratified in trade agreements, and I think it's a bad idea.

DOYLE: Okay, gentlelady's time has expired.

SCHAKOWSKY: Okay, thank you. I yield back.

DOYLE: The Chair now recognizes Mr. Bilirakis, Subcommittee on--Ranking Member of the Subcommittee on Consumer Protection and Commerce, for five minutes.

BILIRAKIS: Thank you, Mr. Chairman, appreciate it. Dr--Mr. Dorsey, you have heard briefly about what I'm hearing from again in my district, my opening remarks. You've heard them.

The other key part with these stories that we're hearing when we conduct these surveys is how we empower law enforcement. In a hearing last year, we received testimony that since 2016, Twitter has intentionally curtailed sharing threat data with law enforcement fusion centers.

Here's the question. You're well aware that on Twitter and Periscope, that traffic has increased from bad actors seeking to groom children for molestation, lure females into sex trafficking, sell illegal drugs, incite violence, and even threaten to murder police officers.

Are you willing to reinstate this corporation retain evidence and provide law enforcement the tools to protect our most vulnerable? Yes or no?

DORSEY: Well, first, child sexual exploitation has no place on our platform and I don't believe that's true.

[*]DORSEY: We work with local law enforcement--

BILIRAKIS: So, you're saying that this is not true? What I'm telling you--are you willing to reinstay--reinstate--in other words, it's not--it's not going on now--reinstate this cooperation with law enforcement to retain evidence and provide law enforcement the tools to protect our most vulnerable?

DORSEY: We would love to work with you in more detail on what you're saying, but we work with law enforcement regularly. We have a strong partnership.

BILIRAKIS: So, you're saying that this is not true what I'm telling you?

DORSEY: I don't believe so, but like--we'd love to understand the specifics.

BILIRAKIS: Would you commit to--to doing what I'm telling you you're not doing in the future, and work with me on this?

DORSEY: We'll continue to doing what we're doing.

BILIRAKIS: And what is that? You're saying that--

DORSEY: --Working with local law enforcement.

BILIRAKIS: Okay. Well, let me go on to the next question, but I'm going to follow up with this to make sure you're doing this. I mean, our chil--children's lives are in jeopardy here. Mr. Zuckerberg, we have heard you acknowledge mistakes about your products before. There are now media reports of an Instagram for under 13 being launched. My goodness. Between this and you two kids--you--you and Mr. Pichai have obviously identified a business case for targeting this age bracket with content, and I find that very concerning, targeting this particular age bracket, 13 and under.

Given these free services, how exactly will you be making money or are you trying to monetize our children too and get them addicted early? And will you be allowing your own children to use this site with a default settings? We're talking about the, again, the--the site that apparently is being launched for children under--13 and under--or under 13, actually. Can you please answer that question for me?

ZUCKERBERG: Congressman, we're early in thinking through how this service would work. There is clearly a--a--a large number of people under the age of 13 who would want to use a service like Instagram. We currently do not allow them to do that. I think to offer a safe--

BILIRAKIS: --What--what would be the purp--what would be beneficial--what would be beneficial for--to our children to launch this kind of service?

ZUCKERBERG: Oh, Congressman, I think helping people stay connected with friends and learn about different content online is broadly positive. There are clearly issues that need to be thought through and worked out, including how parents can control the experience of--of kids, especially kids under the age of 13. And we--we haven't worked through all of that yet so, we haven't formally--

BILIRAKIS: --Appreciate that--

ZUCKERBERG: --announced the plans, but--but I--I think that something like this could be quite helpful for a lot of people.

BILIRAKIS: Excuse me. Okay, my--I'll reclaim my time. Mr. Pichai, your company has had failures curating content for kids. What advice would you offer your colleague here?

PICHAU: Congressman, we've invested a lot in a one-of-a-kind product, YouTube kids. The content there is, you know, we work with trusted content partners. Take Sesame Street as an example of the type of channel you would find there. Science videos and cartoons and we take great effort to make sure--

BILIRAKIS: --I have to reclaim my time. I have one more last--one last question for Mr. Zuckerberg. Do you have concerns with what has appeared on your platform hosted by YouTube? For--and--and, you know, with regard to your children about--in general, do you have concerns, yes or no?

ZUCKERBERG: Congressman, are you asking me about YouTube?

BILIRAKIS: Yes, I'm--I'm asking you about YouTube.

ZUCKERBERG: Con--Congressman, I--I use YouTube to watch educational videos with my children--

BILIRAKIS: --Yeah, do you have concerns, personally for your children and--and your family personally, do you have concerns?

ZUCKERBERG: Congressman, my--my children are five and three years old. So, when--when I watch content on YouTube with them, I'm doing it in supervising them so, in that context, no, I haven't particularly had concerns. But--but I think it's important that, if anyone is building a service for kids under the age of 13 to use by themselves that there are appropriate parental controls.

DOYLE: The gentleman's time has expired.

BILIRAKIS: Thank you.

DOYLE: I'm going to ask all members, too, to try to stick to our five-minute rule so that we can get out of here before midnight. The Chair will now recognize Mr. Pallone, the full committee chair, for five minutes.

PALLONE: Thank you, Chairman Doyle. My questions are of Mr. Zuckerberg and Mr. Pichai. But, you know, I just want to say, after listening to the two of yours' testimony, you definitely give the impression that you don't think that you're actively, in any way, promoting this mis--misinformation and extremism. And I totally disagree with that. You're not passive bystanders, you're not, you know, nonprofits or religious organizations that are trying to do, you know, a good job for humanity.

You're making money. And the point we're trying to make today--or at least I am--is that, when you spread this information, actually--misinformation extremism--active--actively promoted and amplify it, you do it because you make more money. And so, I, you know, I kind of deny the basic premise of what you said. But, let me get to the questions. Let me ask Mr. Zuckerberg, according to a May 2020 Wall Street Journal report, a Facebook researcher concluded that Facebook's own recommendation tools were tied to a significant rise in membership in extremists Facebook groups in Germany.

I wrote to you last month requesting this research and related documents. I trust you'll fully cooperate with the committee's inquiry and provide all requested documents and information. But my question is--and please, yes or no--were you aware of this research showing that 64 percent of the members in the extremist Facebook group's study joined because the Facebook's own recommendations tool--joined these extremist groups in--in Germany. Were you aware of that, yes or no?

ZUCKERBERG: Congressman, this is something that we've studied because we want to make sure our products improve--

PALLONE: --But I'm asking if you were aware of it. It's a simple question, yes or no? Were you aware of it, that's all I'm asking. Were you aware of this res--

ZUCKERBERG: --Where--at--at what time? After--after we studied--

PALLONE: --I didn't ask that, I just asked if you were aware of it, Mr. Zuckerberg, yes or no? If not, I'm going to assume that the answers yes, okay?

ZUCKERBERG: Congressman, I've seen--I've seen the study. It--it was about a--a--content leading up to the German election--

PALLONE: --I appreciate that--

ZUCKERBERG: --and we--we've since made changes to the platform.

PALLONE: Let me go to the second question which relates to that. You said, yes, okay. The troubling research I mentioned demonstrates that Facebook was not simply allowing disinformation and extremism to spread, it actively amplified it and spread it. This is my point. Nonetheless, Facebook didn't permanently stop recommending political and civil groups to the United States until after the January 6 insurrection years after it was made aware of this research. The fact that Facebook's own recommendation system helped populate extremist groups compels us to reevaluate platforms' liabilities.

Now, back to that Wall Street Journal article, Facebook's chief product Officer, Chris Cox, championed an internal effort to address division on Facebook and proposed a plan that would have reduced the spread of content by hyperactive users on the far left and far right. The article alleges, Mr. Zuckerberg, that you personally reviewed this proposal and approved it, but only after its effectiveness was--was decreased to 80 percent. Is that true, yes or no, please?

ZUCKERBERG: Congressman, we've--we've made a lot of--of measures that aim to fight this content, including--

PALLONE: --Did you approve that--

ZUCKERBERG: --Sorry--

PALLONE: --Did you approve after its effectiveness was decreased to 80 percent, yes or no?

ZUCKERBERG: Congressman, I--I can't speak to that specific example, but we put in place a lot of different measures and in the aggregate, I think that they're effective, including--

PALLONE: --You did--did you review the proposal and approve it?

ZUCKERBERG: Congressman, we do a lot of work in this area and I review a lot of proposals. We've moved forward on a lot of steps--

PALLONE: --It's not a difficult question. I'm just asking if you reviewed this internal proposal and you approved it. And you won't even answer that. I don't--it so easy to answer that question. It's very specific. All right, you won't answer, right, yes or no?

ZUCKERBERG: Congressman, that's not what I said. I--I said I did review that, in addition to many other proposals and things that we've taken action on, including shutting off recommendations for civic and political groups--

PALLONE: --You said you reviewed it. We'll prove it with the 80 percent decrease in effectiveness.

ZUCKERBERG: Congressman, I--I don't remember that specifically, but we've taken a number of different steps on--on this--

PALLONE: --Okay. Fine, let me go to Mr. Pichai. Mr. Pichai, according to the New York Times, YouTube's recommendation algorithm is responsible for more than 70 person--70 percent of the time users spend on YouTube. In fact, a former design ethicist at Google was quoted as saying, "If I'm YouTube and I want you to watch more, I'm always going to steer you towards crazy town." Mr. Pichai, is mis--is YouTube's recommendation algorithm designed to encourage users to stay on the site, yes or no? Is it designed to encourage users to stay on the site, yes or no?

PICHA: Content response and release are our number one goals so that--

PALLONE: I am asking very simple whether you recognize--YouTube's recommendation algorithm is designed to encourage users to stay on the site--simple question, yes or no?

PICHAU: That's not the sole goal, Congressman. We definitely--

PALLONE: So the answer is yes. OK. So the bottom line is simply put, your company's bottom line compel you to amplify extremist and dangerous content. You're not bystanders and what happens on that--online doesn't stay online. It has real-world consequences. That's why Congress has to act because you're not bystanders. You're encouraging this stuff. Thank you, Mr. Chairman.

DOYLE: Gentleman's time is expired. The Chair now recognizes Ms. Rodgers, the full committee ranking member for five minutes.

RODGERS: We've tragically lost number of young people to suicide in my community. In a three year period from 2013 to 2016, the suicide rate more than doubled in Spokane County. In the last six months, one high school lost three teens. Right now, suicides the second leading cause of death in the entire state of Washington for teens 15 to 19 years old. As I mentioned, it's led to many painful conversations, trying to find some healing for broken families and communities. And together, we've been asking, what's left our kids with a deep sense of brokenness?

Why do children, including kids we've lost in middle school feel so empty at such a young, vulnerable age? Well, some studies are confirming what parents in my community already know--too much time on screens and social media is leading to loneliness and despair. And it seems to be an accepted truth in the tech industry. Because what we're hearing today, making money is more important.

Bill Gates put a--put a cap on screen time for his daughter. Steve Jobs once said in a quote, we limit how much technology our kids use at home. Mr. Zuckerberg, you've also that your kids--that you don't want your kids sitting in front of screens passively consuming content. So, Mr. Zuckerberg, yes or no, do you agree too much time in front of screens passively consuming content is harmful to children's mental health?

ZUCKERBERG: Congresswoman, the research that I've seen on this suggests that if people are using computers and--and social apps--

RODGERS: Could you use yes or no? I'm sorry. Could you use yes or no?

ZUCKERBERG: I--I don't think that the research is conclusive on that. But I--I can summarize what I've learned if that's helpful.

RODGERS: I will--I'll follow up at a later time because I--I do know that Facebook has acknowledge that passive consumption on your platform is leading to people feeling worse. And we've said that going from video to video is not positive. Yet, Facebook is designed to keep people scrolling--Insta--Instagram is designed to get users to go from video to video. So I would like to ask you if you--if you said earlier that you don't want kids sitting in front of the screens passively consuming content and your products are designed to increase screen time, do you currently have any limitations on your own kids use of your products or--or how do--how do you think that will change as they get older?

ZUCKERBERG: Sure. Congresswoman my--my daughters are five and three and they don't use our products. Actually, that's--that's not exactly true. My eldest daughter, Max, I let her use Messenger Kids sometimes to message her cousins.

But overall the--the research that we've seen is that using social apps to--to connect with other people can have positive mental health benefits and well-being benefits like helping people feel more connected and less lonely. Passively consuming content doesn't have those positive benefits to well-being but isn't necessarily negative but just isn't as positive as connecting.

And the way we design our algorithms is to encourage meaningful social interactions. So it's a common misconception that our teams our--our goal or even have goals of trying to increase the amount of time that people spent. The newsfeed team at Facebook and the Instagram team--

RODGERS: Thank you. Mr. Zuckerberg, I do have a couple of more questions. So do you agree that your business model and the design of your products is to get as many people on the platform as possible and to keep them there for as long as possible if you could answer yes or no that would be great.

ZUCKERBERG: Congresswoman, from a mission perspective, we want to serve everyone. But our goal is not we don't--I don't give our newsfeed team, our Instagram team goals around increasing the amount of time that people spend. I believe that if we build a useful product which--

RODGERS: OK. Thank you. Thank you. We all have limited time. Think the business model suggests that it is true. It was mentioned earlier that your studying extremism. I'd like to ask yes or no of all of you beginning with Mr. Zuckerberg, has Facebook conducted any internal research as to the effect your products are having on the mental health of our children?

ZUCKERBERG: Congresswoman, I know that this is something that we--that we try to study and understand.

RODGERS: Can you answer yes or no? I'm sorry.

ZUCKERBERG: I believe the answer is yes.

RODGERS: OK. Mr. Dorsey, has Twitter?

DORSEY: I don't believe so but we'll follow up with you.

RODGERS: OK. Mr. Pichai, has Google conducted any research on the effect your products are having on the mental health of children?

PICHAJ: We consult widely with expert third parties on this area including SAMHSA and other mental health organizations and invest a lot of time and effort in this area.

RODGERS: OK. I would like to see that it--it sounds like you've--you've studied extremism let's get focused on our (INAUDIBLE).

DOYLE: Gentlelady's time has expired. The Chair now recognizes Mr. Rush for five minutes. Bobby, you need to unmute. There you go. Nope. You're still muted.

RUSH: I want to thank you, Mr. Chairman. We all agree that social media sites (INAUDIBLE) for stoking racial division or exacerbating racial injustices. However, there is a growing body of research that demonstrates the disproportionate effects of disinformation and white supremacist extremism on women and people of color, especially black people.

We have seen and continue to see that too often social media sites put their earnings before equality. Simply stated you--your corporations carelessly put profits over people. Misinformation, awareness (INAUDIBLE) conspiracy theories and incery--incendiary content targeting minorities remains (INAUDIBLE). And social media companies, your companies are profiting from hate and racism on these platform--platforms by harnessing (INAUDIBLE) and generating (INAUDIBLE) revenue from such content.

There is only one comparison and that remotely approaches the (INAUDIBLE) immoral, (INAUDIBLE) of your companies and that--that is the (INAUDIBLE) of our nation's shameful and inhumane and--and--and--and most (INAUDIBLE) in the past. This is--this is the very reason why I ask Mr. Dorsey, I remember you at our 2018 hearing to commit to commissioning an independent third-party civil rights audit on Twitter. This request at the hearing was followed up with my joint letter from Chairman Pallone and myself confirming that commitment. It is three years later. And I am still waiting , Mr. Dorsey, for the results of that audit.

Where is that audit, Mr. Dorsey?

DORSEY: Thank you. We--we--we've taken another approach which is to work with civil rights orgs on a regular basis. We have regular conversations with civil rights orgs multiple times a year.

RUSH: Where is--where is the audit? Members from Congress, including the Chairman of the committee where is the audit that we asked you and you agreed to forward?

DORSEY: We--we don't have it. we thought a different approach was--

RUSH: I don't have--I--I have not I don't have it either and I thought you were being very, very dis-ingenuine. As a matter of fact, I thought that you had intentionally lied to the committee and you should be condemned for that and I can't wait until we come up with legislation that will review you and your cohorts in a very, very expensive way. This was nothing but an empty promise that you made. (INAUDIBLE) and concerns me. Mr. Dorsey, I as black man in America, my experiences are different from your experiences. These--and this audit is very, very important to me and to those who are similarly situated just as I am.

Facebook, (INAUDIBLE) has completed an audit and there's no reason, simply on reason (INAUDIBLE) corporations, (INAUDIBLE) yours, should not completed that audit.

Mr. Dorsey, has Twitter evaluated the disparate impact from COVID-19 (INAUDIBLE) misinformation (INAUDIBLE) on the African American community? And, secondly, has the company even attempted to identify methods to combat COVID-19 misinformation targeting African Americans and reliable, trustworthy vaccine information?

DORSEY: Yes on both and we review with civil rights groups directly on a regular basis. That is the solution we chose.

DOYLE: The gentleman's time has expired. Chair now recognizes Mr. Upton for five minutes.

UPTON: Well, thank you, Mr. Chairman. You know, as I listen to this hearing, like it or not, it sounds like everybody on both sides of the aisle is not very happy. I think we all believe that there is a lot of responsibility that should be shared for some of the issues that we've raised today by the three of you, and I would just offer--or speculate, I guess you could say, that we're going to see some changes in Section 236--230.

You know, the president--former president Trump vetoed a pretty big bill, the Defense bill, earlier last year over this very issue because he wanted the total repeal and he didn't get it. But, I know that the Senate now has got some legislation that's pending that's looking at a couple reforms and my sense is that we may see something here in the near future as well.

I serve on--as one of only two House members on the Commission on Combatting Synthetic Opioids Trafficking. It's a multi-federal agency. It's co-chaired by David Trone in the House and Tom Cotton in the Senate. And, there is a lot of concern that we all have, not only as parents, but as community leaders across the country on opioids and the inability to remove illegal offers of opioids, steroids, even fake COVID-19 vaccines, very troubling I think as we see some of these platforms push such content to a user in real search of it.

So, I guess my first question is to you, Mr. Zuckerberg. The sale of illegal drugs on your platform does violate your policy yet it does remain a problem on your platform. Can you explain the resources that you currently have devoted to addressing the issue and whether or not you plan to devote more? And, I--this is an issue that I intend to raise with the--with the Commission as we look forward to this in the next number of months.

ZUCKERBERG: Thanks, Congressman. I think this is an important area and a good question. We have more than 1,000 engineers who work on our--our, what we call integrity systems that basically are AI systems that try to help find content that violates our policies. You're right that that content does violate our policies, and we also have more than 35,000 people who work in content review who basically are either responding to flags that they get from the community or--or checking things that our AI systems flag for them but aren't sure about.

And, this is an area--and when we're talking about reforming Section 230--where I think it would be reasonable to expect that large platforms especially build effective systems to be able to combat and fight this kind of clearly illegal content. I think that there will be a lot of ongoing debate about how to handle content which people find distasteful or maybe harmful but is legal. But, in this case, when the content is illegal, I think it is pretty reasonable to expect that large platforms build effective systems for moderating this.

UPTON: So, we saw earlier this week--of course, we don't know all the facts on this terrible shooting in Boulder, Colorado. It appears, in at least some of the initial reports, that the alleged shooter was in fact bullied and I think I saw some press reports that some of it had happened online as well. What--what process do you have to--that would allow parents or families to be able to pursue anti-bullying efforts that might be on your platform?

ZUCKERBERG: Thanks, Congressman. I think bullying is--is a really important case to consider for Section 230 because first of all, it's horrible and we need to fight it and we have policies that are against it. But, it also is often the case that--that bullying content is not clearly illegal.

So, when we talk about needing the ability, under something like Section 230, to be able to moderate content, which is not--not only clearly illegal content, but broader, one of the primary examples that we--that we have in mind is making sure that we can stop people from bullying children. You know, here, we work with--with a number of advocacy groups. We work with law enforcement to help fight this. This is a huge effort and--and part of what we do and I think it's extremely important.

UPTON: And, other than taking the approach that you don't want to see any changes to 230, what suggestions might you have for us as we examine this issue?

ZUCKERBERG: Sorry, Congressman, I'm not saying that I don't think that there should be changes. I'm saying that I think 230 still broadly is important, so I wouldn't repeal the whole thing. But, the three changes that I've basically suggested are one is around transparency, that large platforms should have to report on--on a regular cadence for each category of harmful content, how much of that harmful content they're finding and how effective their systems are at dealing with it.

The second thing I think that we should do is hold large platforms to a standard where they should have effective systems for handling clearly illegal content, like opioids, or child exploitation or things like that. And, the third thing that I think is an important principle is that these policies really do need to apply more to large platforms and I think we need to find a way to exempt small platforms so that way, you know, when I was getting started with Facebook, if we had gotten hit with a lot of lawsuits around content, it might have been prohibitive for me to get started and I think none of us want to see--

UNKNOWN: --(INAUDIBLE)--

ZUCKERBERG: --the next set of platforms from being stopped from--from kind of being able to get started and grow.

DOYLE: The gentleman's time has expired. Chair now recognizes Ms. Eshoo.

ESHOO: Am I unmuted? Thank you, Mr. Chairman, and good morning. Well, it's still--we're in California, so it's good morning for us.

I want to start by saying that content moderation, like removing posts or banning accounts, is about treating symptoms and I think that we need to treat symptoms, but I also think that we need to address two underlying diseases. The first is that your products amplify extremism. The second is that your business models of targeted ads enable misinformation to thrive because you chase user engagement at great costs to our society.

So, to Mr. Pichai, last month, the Anti-Defamation League found that YouTube amplifies extremism. Scores of journalists and researchers agree and here's what they say happens. A user watching an extremist video is often recommended more such videos, slowly radicalizing the user.

YouTube is not doing enough to address recommendations and it's why Representative Malinowski and myself introduced the Protecting Americans From Dangerous Algorithms Act to narrowly amend Section 230 so courts can examine the role of algorithmic amplification that leads to violence, and it's also why I, along with 40 of my House colleagues, wrote to each of you about this issue. And, Mr. Chairman, I ask that those letters be placed into the record.

So, my question to you, Mr. Pichai, is are you willing to overhaul YouTube's core recommendation

[*]ESHOO: to correct this issue, yes or no?

PICHAJ: Congresswoman, we have overhauled our recommendation systems--and I know you've engaged on these issues before--pretty substantially in pretty much any area--

ESHOO: --Mr. Pichai, yes or no, because we still have a huge problem. And I--I outlined what they--are you saying that the Anti-Defamation League doesn't know what they're talking about? You know, all these journalists and researchers, there is a lot more to address. And that's why I'm asking you if you're willing to overhaul YouTube's core recommendation engine to correct this. It's serious, it's dangerous, what more can I say about it? Yes or no?

PICHAJ: Congresswoman, if I may explain, we have--

ESHOO: --No, I don't have time to explain. So, we--you know, let me just say this to--to the witnesses, we don't do filibusters in the house. That's something that's done in the Senate. So, a filibuster doesn't work with us. To Mr. Zuckerberg, your algorithms use unseemly amounts of data to keep users on your platform because that leads to more ad revenue. Now, businesses are in business to make money, we all understand that. But your model has a cost to society. The most engaging posts are often those that induce fear, anxiety, anger, and that includes deadly--deadly misinformation.

The Center for Countering Digital Hate found that the explore and suggested posts parts of Instagram are littered with COVID misinformation, election disinformation, and QAnon posts. So, this is dangerous and it's why Representative Schakowsky and I are doing a bill that is going to ban this business model of surveillance

advertising. So, are you willing to redesign your products to eliminate your focus on addicting users to your platforms at all costs, yes or no?

ZUCKERBERG: Congresswoman, as I said before, the teams the design our algorithms and especially--

ESHOO: --You know what, I think--let me just say this, and it's--I think it's irritating all of us, and that is that no one seems to know the word yes or the word no. Which one is it? If you don't want to answer, just say I don't want to answer. So, yes or no?

ZUCKERBERG: Congresswoman, these are nuanced issues--

ESHOO: --Okay, I'm going to say that's a no. To Mr. Dorsey, as chairwoman of the health subcommittee, I think that you need to eliminate all COVID misinformation and not label or reduce its spread, but remove it. I--I looked at a tweet this morning--Robert Kennedy Jr. links the death of baseball legend, Hank Aaron, to the COVID vaccine, even though fact-checkers debunked the story. The tweet has 9000 retweets. Will you take this down? And why haven't you? And also, why having you band the 12 accounts that are spewing it's deadly COVID misinformation? This could cost lives.

DORSEY: No--no, we won't take it down because it didn't violate our policy. So, we have a clear policy in place--

ESHOO: --What type of policy is that? Is it a policy for infor--misinformation?

DORSEY: No.

DOYLE: The gentlelady's time has expired. The Chair recognizes Mr. Scalise. Is Mr. Scalise here?

SCALISE: Thank you.

DOYLE: Ah, there we go.

SCALISE: Yeah, thank you, Mr. Chairman. I want to thank you for having this hearing. I want to thank our three witnesses for coming as well. Clearly, you're seeing a lot of concern being expressed by members on both sides, both Republican and Democrat, about the way that your social media platforms are run, and especially as it relates to the fairness and equal treatment of people.

I know I've had a lot of concerns shared with some of you, individually, over the last few years about whether it's algorithms that seem to be designed, some time, to have an anti-bias against conservatives. But, look, we all agree that whether it's illegal activity, bullying, those things ought not be permeated through social media. But there's a big difference between stopping bullying and violent type of social media posts versus actual censorship of political views that you disagree with.

And--and I think--I want to ask my first question to Mr. Dorsey because there have been a lot of concerns expressed recently about that unequal treatment and--and I'll just start with the New York Post article. I think a lot of people have seen this. This article was censored by Twitter when it was originally sent out. This is the New York Post, which is a newspaper that goes back to 1801, founded by Alexander Hamilton. And for weeks, this very credibly sourced article, right before an election, about Hunter Biden, was--was banned by Twitter.

And then, when you contrast that, you have this Washington Post article that was designed to mis-portray a conversation between President Trump and the Georgia Secretary of State--since been--parts of this have been debunked. And, yet, this this article can still be tweeted out. I went to ask Mr. Dorsey, first of all, do you recognize that there is a real concern that there is an anti-conservative bias on Twitter's behalf? And do you recognize that this has to stop? This is going to be--Twitter is going to be viewed by both sides as a--as a place where everybody's going to get a fair treatment.

DORSEY: We--we made a total mistake with the New York Post. We corrected that within 24 hours. It was not--it was not to do with the content, it was to do with the hacked materials policy. We had the incorrect interpretation. We--we don't write policy according to any particular political leaning. If we find any of it, we write it out.

SCALISE: So, regarding the Washington Post--

DORSEY: --We make mistakes--we will make mistakes. And our--our goal is to correct them as quickly as possible and, in that case, we did.

SCALISE: And--and I appreciate you recognizing that was a mistake. However, the New York Post's entire Twitter account was blocked for about two weeks where they couldn't send anything out, not just that article. And to censor--we've got a First Amendment too--it just seems like to censor a newspaper that's as highly respected as the New York Post, again, 1801 founded by Alexander Hamilton--for their entire account to be blocked for two weeks by a mistake seems like a really big mistake. Was anyone held accountable in--in your censoring department for that mistake?

DORSEY: Well, we don't have a sensory department. But I--I agree--like it did--

SCALISE: --Well, who made the decision then to block their account for two weeks?

DORSEY: We--we didn't block their account for two weeks. We required them to delete the tweet and then they could tweet again. They didn't take that action so, we corrected it for them. That was--that--

SCALISE: --Even though the tweet was accurate. I mean, argue--are you now--look, you've seen the conversations on both sides about Section 230 and there's going to be more discussion about it, but your acting as a publisher. If you're telling a newspaper that they've got to delete something in order for them to be able to participate in your account, I mean, don't you recognize that that--you're no longer hosting the town square, your acting as a publisher when you do that.

DORSEY: It was--it was, literally, just a process error. This was not against them in any particular way. We require, if we remove a violation, we require people to correct. We changed that based on their not wanting to delete that tweet. I completely agree with--I see it--but it is--it is something we learned, like we learned--

SCALISE: --Okay, let me go to the New York--now let me go to the Washington Post article because this article can still be tweeted. I don't know if it was ever taken down. It contains false information, even the Washington Post acknowledges that it contains false information, yet, there are tweets today on your service that still mischaracterize it in a way where even the Washington Post admitted it's wrong. Yet, those mischaracterizations can still be retweeted. Will you address that and start taking those down to reflect what even the Washington Post themselves has admitted as is false information?

DORSEY: Our--our misleading information policies are focused on manipulated media, public health, and civic integrity. That's a--we don't have a--

SCALISE: --I--I would hope that you would go in and take that down. And, look, I know you said in your opening statement, Mr. Dorsey, that Twitter is running a business. And you said, "A business wants to grow its customer--the customers it serves." Just recognize, if you become viewed--and continue to become viewed as an anti-conservatively biased platform, there will be other people that step up to compete and ultimately take millions of people away from Twitter--

BUTTERFIELD: --Our turn--

SCALISE: --I would hope you recognize that. And I would yield back the balance of my time.

DOYLE: The gentleman's time has expired. The Chair now recognizes Mr. Butterfield for five minutes.

BUTTERFIELD: Thank you, Mr. Chairman. Mr. Zuckerberg, last year, in response to the police killing of George Floyd, you wrote a post on your Facebook page that denounced racial bias. It proclaimed, "black lives matter." You also announced that the company would donate \$10 million to social justice organizations. And, Mr. Dorsey, Twitter changed its official bio to a Black Lives Matter tribute and you pledged \$3 million to antiracism organization started by Collin Kaepernick. And Mr. Pichai, you--your company held accompany wide moment of silence to honor George Floyd and you announced \$12 million in grants to racial justice organizations. The CEO of Google subsidiary, YouTube, wrote in a blog post, "We believe black lives matter and we all need to do more to dismantle systemic racism." End of quote. YouTube also announced it would start a \$100 million fund for black creators. Now, all of this sounds nice but these pronouncements, gentleman, these pronouncements and money donations do not address the way your companies own products--Facebook, Twitter and YouTube have been successfully weaponized by racists and are being used to undermine social justice movements to suppress voting in communities of color and spread racist content and lies.

So gentleman in my view--in my view your companies have contributed to the spread of race based extremism and voter suppression. As The New York Times noted last year, "It's as if the heads of McDonalds, Burger King and Taco Bell all got together to fight obesity by donating to a vegan food co-op rather than lowering their calories," end of quote.

Gentleman, you could have made meaningful changes within your organizations to address the racial biases built into your products--and donated to these organizations. But instead, we are left with plentitudes and another round of passing the buck. America is watching you today. This is a moment that begins a transformation of the way you do business and you must understand that. Perhaps a lack--lack of diversity within your organizations has contributed to these failures. The Congressional Black Caucus Tech 2025 Initiative has been working for years to increase diversity and equity in tech companies at all levels and you know that because we have visited with you in California.

We have founded this initiative in 2015 with the hope that by now the tech workforce would reflect the diversity of our country. Here we are, 2021, I acknowledge that you have made some modest advancements--but not enough. There must be meaningful representation in your companies to design your products and services in ways that work for all Americans. And that requires public accountability. History has shown that you have talked the talk but have failed to walk the walk. It appears ow that Congress will have to compel you--compel you perhaps with penalties to make meaningful changes.

And I'm going to try the yes or no answer and hopefully, I will have better results than my colleagues. Mr. Zuckerberg, I'll start with you and please be brief yes or no--would you oppose legislation that would require technology companies to publicly report on workforce diversity at all levels?

ZUCKERBERG: Congressman, I don't think so but I need to understand it in more detail.

BUTTERFIELD: Well, we've talked about that and I hope that if we introduce this legislation you will not oppose it. What about you, Mr. Dorsey--would you oppose a law that make workforce diversity reporting a requirement?

DORSEY: No. I wouldn't oppose it. It--it does come with some complications in that we don't always have all the demographic data for all our employees.

BUTTERFIELD: Well, thank you for that and we talk with you in your office some years ago and you made a commitment to work with us. But we need more. What about you, Mr. Pichai are you willing to--to support--well, would you be willing to commit to a--to a would you oppose a law that make workforce diversity reporting a requirement? Would you oppose it?

PICHAJ: Congressman, we were the first company to publish transparency reports. We publish it annually and so happy to share that with you and take any feedback and what we do today provide in the U.S. detailed demographic information on our workforce and we are committed to doing better.

BUTTERFIELD: Gentleman, for the last six years--the Congressional Black Caucus has said to you over and over again we need greater diversity among your workforce from the top to the bottom and we need for you to publish the data so the world can see it. That is the only way we are going to deal with diversity and equity. Thank you so very much, Mr. Chairman. I heard you at the beginning of the committee gavel and I yield back the 10 seconds that I have.

DOYLE: Gentleman deserves a commendation for doing that and I hope others follow his example. Chair now recognizes Mr. Guthrie, for five minutes.

GUTHRIE: Thank you, Mr. Chair and thanks to the witnesses for being here. Big tech--big tech decisions have real impact on people and that's why as my constituents using your platforms to share their experiences on your platforms with me as their representative and I am here to advocate on their behalf.

I received 450 responses and one major thing that I heard from my constituents was the experience they had with sites taking down religious content. Which is important because there's a lot of religious organizations who are now streaming their services due to COVID. I did have one instance where a constituent wrote to me quote, and this is what she posted, "I am thankful God's grace is new every morning." And then, Facebook took it down. And then, my constituent said she got a notice from Facebook that it violated their policies around hate.

And so, I just wanted to discuss about this. I can ask you yes or no questions Mr. Zuckerberg on that and--and but I just want to talk about it a little bit. It just seems--I know that we--we don't want extreme language on the internet. I'm--I'm with you on that. And you can't watch everything. And so, you use algorithms to find it. So algorithms will flag things. Some that are clearly obvious and some that you will say probably shouldn't have been flagged.

But it--it seems to me that it--it seems to be bias in that direction. So instead of just giving you a yes or no question I want to read that quote again and I know a little bit about math--not a lot, but a little bit, about within that quote what in there would get tripped up and would this quote get tripped up and put into the flag category and she says, I'm thankful God's grace is new every morning. So my question is what word or thought do you think would trip a--an algorithm for that--that quote, Mr. Zuckerberg.

ZUCKERBERG: Congressman, it's--it is not clear to me why that post would be--would be a problem. I--I would need to look into it in--in more detail. Sometimes the systems look at patterns of--of postings of someone is posting a lot then maybe our system thinks it's spam but I would need to look into it in more detail.

Overall, I mean the--the reality is is that any system is going to make mistakes. There's going to be content that we take down that we should have left up and there's going to be content that we missed that we should have taken down that we didn't catch or that the systems made a mistake on. And at scale, unfortunately, you know, those mistakes can be a large number even if it's a very small percent.

That's why when we're talking about things like Section 230 reform I--I think it is reasonable to expect large companies to have effective moderation systems but not reasonable to expect that there are never any errors. But--but I think that transparency can help hold the companies accountable as to what accuracy and--and effectiveness they're--they're achieving.

GUTHRIE: OK. Thank well to your spam comment I think they did receive a notification it was for the hate policy so and--and I understand there's going to be gray areas whatever that--that quote I don't see where the gray area is and how it could get caught up in that. But (INAUDIBLE) thanks for your answer with that.

I want to move on. So, Mr. Dorsey, I want to talk about the RFK Jr. I didn't see that quote, but you said that didn't violate your policy. And--and just in the context of that I know CDC just recently updated its school guidance. To make clear, science says you can be three feet away and still be safe in schools. The issue--things are changing every day cause we're learning more and more about this virus. So how did the RFK comment not violate your policy and RFK Jr. and how did--we have a RFK III that we all and JFK and JPK III I guess we all like and as a former colleague--but RFK Jr. and the policy towards that and then, how do you keep up with what's changing so quickly--Mr. Dorsey?

DORSEY: We can--we can follow-up with you on the exact reasoning but I the--we have to recognize that our policies evolve constantly and they have to evolve constantly so as--as been said earlier in this--in this testimony we--we observe what's happening as a result of our policy. We got to understand the ramifications and we--we improve it. And it is a constant cycle. We are always looking to improve our policies and our enforcement.

GUTHRIE: So, Mr. Zuckerberg, Mr. Pichai just on all that--continuously evolving information on COVID because we are learning more and more about it and how do you keep it. We only have about 30 seconds if you could a quick answer for each of you--if you can. Mr. Pichai maybe since you haven't talked--asked--answered a question.

PICHAU: On--on COVID, we have been really taking guidance from CDC and other health experts proactively removing information. One thing we get to do in YouTube is to recommend higher-quality content.

[*]PICHAU: We have shown over 400 billion information panels on COVID alone last year, including a lot from CDC and other health organizations.

GUTHRIE: Okay, thank you and I'll yield back four seconds, Mr. Chair.

DOYLE: Thank you, Mr. Guthrie. Chair now recognizes Ms. Matsui for five minutes.

MATSUI: Thank you very much, Mr. Chairman, for having this hearing today. Today, we have another opportunity here for the leaders of Facebook, Twitter, and Google, and one has become a concerning pattern. The members of this committee are here to demand answers to questions about social media's role in escalating misinformation, extremism and violence.

Last week, I testified at a House Judiciary committee hearing about the rise in discrimination and violence against Asian-Americans. Horrifically, that hearing came on the heels of a violent attack in Atlanta that left eight people, six of whom were Asian women, dead.

The issues we are discussing here are not abstract. They have real-world consequences and implications that are too often measured in human lives. I'm worried, as are many watching this hearing, that the companies before us today are not doing enough to prevent the spread of hate, especially when it's targeted against minority

communities. Clearly, the current approach is not working and I believe Congress must revisit Section 230.

A recent study from the University of San Francisco examined nearly 700,000 tweets in the week before and after President Trump tweeted the phrase "Chinese virus." The results showed two alarming trends. There was a significantly greater increase in hate speech the week after the president's tweet and that half of the tweets using the hashtag "China virus" showed an anti-Asian sentiment compared to just one-fifth of the tweets using the hashtag COVID-19.

This empirical evidence backs up what the World Health Organization already knew in 2015, saying disease names really do matter. We've seen certain disease names provoke a backlash against members of particularly religious or ethnic communities. Despite this, Facebook and Twitter are still allowing hashtags like "China virus," "Hungflu," and "Wuhan virus" to spread.

Mr. Zuckerberg and Mr. Dorsey, given the clear association between this type of language and racism and violence, why do you still allow these hashtags on your platforms? Any--anyone want to answer that or is that not answerable?

DORSEY: I think we were waiting for you to call on one of us. We--we do have policies against hateful conduct and that includes the trends. So, when we see associated with any hateful conduct, we will take action it. It's useful to remember that a lot of these hashtags do contain counter speech and people on the other side of it do own them and--and show why this is so terrible and why it needs to stop.

MATSUI: Can I just take my time back? The fact of the matter is, is I think you know how to develop algorithms to kind of get rid of this and examine this further. Mr. Zuckerberg, any comment here?

ZUCKERBERG: Thanks, Congresswoman. The--the rise in anti-Asian hate is a really big issue and something that I do think that we need to be proactive about. The--and I agree with the comments that Jack made on this.

You know, any--on Facebook, any of that context, if it's combined with something that's clearly hateful, we will take that down. It violates the hate speech policy. But, one of the nuances that Jack highlighted that we certainly see as well, in enforcing hate speech policy, is that we need to be clear about when someone is saying something because they're using it in a hateful way versus when they're denouncing it. And, this is one of the things that has made it more difficult to--to stop (INAUDIBLE) at scale.

MATSUI: (INAUDIBLE) an opportunity to really look at hate speech and what it really means, particularly in this day and age when we have many instances of these things happening. You know, hate speech on social media can be baked in and unfortunately, this also is a trend that maybe happened years and years ago, in which it might have just been a latent situation.

But, with social media, it travels all around the world and it hurts a lot of people and my feeling--and I believe a lot of other people's feeling--is that we really have to look at how we define hate speech and, you know, you all are very brilliant people and you hire brilliant people. I would think that there is a way for you to examine this further and take it one step lower to see if it is something that it is legitimate or not, and I really feel that this is a time, especially now when we're examining platforms and what you can do and should do, and as we're examining here in this committee and as we write legislation, we really want to have the entire multitude of what can and can't be done.

So, with that, Mr. Chairman, I only have 12--11 seconds left and I yield back. Thank you.

DOYLE: Thank you. Gentledady yields back. Let's see. The Chair now recognizes Mr. Kinzinger for five minutes.

KINZINGER: Thank you, Mr. Chairman, and thank you all for being here. You know, in all this conversation, it's good to have--I think we also have to recognize that we need to--we're lucky to have all these companies located in the United States. You know, when we talked about the issues and concerns, for instance, with TikTok, we can see that a lot of these companies could easily leave here and go elsewhere and then we would have far less oversight.

I think the crackdown on January 6th was correct. I think we need to be careful to not use that as a way to deflect from, you know, what led to January 6th, you know, pushing of this narrative of Stop the Steal. I think there are folks that are concerned, though, that we also need to make sure that those same levels of protection exist when you talk about, like, Iran, for instance and what the leaders there tweet.

But, let me go into specific questions. So, over the years, we've obviously seen the rise of disinformation. It's not new. I remember getting disinformation in the '90s, but we've seen it spread on these platforms. We live in a digital world where many people get their news and their entertainment from the internet from articles and posts that are often based off algorithms that can cater to what people see and read.

So, with those constant newsfeeds, it simply reinforces people's beliefs or worse, that they can promote disgraceful and utterly ridiculous conspiracy theories from groups like QAnon. Extremism and violence have grown exponentially as a result and we know it's true specifically after January 6th.

So, Mr. Zuckerberg, let me ask you. According to Hany Farid at Berkeley, numerous external studies and some of your own internal studies have revealed that your algorithms are actively promoting divisive hateful and conspiratorial content because it engages users to spend more time. Do you think those studies are wrong? And, if--if not, what are you guys doing to reverse course in that?

ZUCKERBERG: Sure. Thank you, Congressman. This is an important set of topics. In terms of groups, we stopped recommending all civic and political groups, even though I think a lot of the civic and political groups are healthy, because we--we were seeing that that was one vector that--that there might be polarization or extremism and groups might start off with one, you know, set of views but migrate to another place. So, we removed that completely and we did it first as an exceptional measure during the election and since the election, we've announced that we're going to extend that policy indefinitely.

For the rest of the content and newsfeed and on Instagram, the--the main thing that I'd say is I do think that there's quite a bit of misperception about how our algorithms work and what we optimize for. I've heard a lot of people say that, you know, we're optimizing for keeping people on the service.

The way that we view this is that we are trying to help people have meaningful social interactions. People come to social networks to be able to connect with people. If we deliver that value, then it will be natural that people use our services more, but that's very different from setting up algorithms in order to just kind of try to tweak and optimize and get people to spend every last minute on our service, which is not how we--how we designed the company or the services.

KINZINGER: Thanks, I didn't mean to interrupt you. I just, I do have another question. Mr. Chairman, I want to ask unanimous consent to insert to the record an article from The Wall Street Journal titled Facebook Executive Shut Down Efforts to Make the Site Less Divisive.

Let me move onto the next one. For years, I've called for increased consumer protection from companies on fake accounts and bad actors who use them to exploit others. This issue affected me personally in 2015. A woman from India spent all of her money on a flight to come see me because she claimed to have developed a relationship with me over Facebook.

In 2019, I sent you, Mr. Zuckerberg, a letter highlighting the issue and your team provided a relatively inadequate response. Since then, I've introduced two pieces of legislation, Social Media Accountability and Account Verification Act and the Social Media Fraud Mitigation Act, both of which aim to curb this activity.

So, Mr. Zuckerberg, the last time you came before us, you stated that Facebook has a responsibility to protect its users. Do you feel that your company is living up to that? And, further, what have you done to remove those fake accounts?

ZUCKERBERG: Thanks. So, fake accounts are one of the bigger integrity issues that we face. I think in the first half of--or--in the last half of last year I think we took down more than a billion fake accounts just to give you a volume--a sense of a volume. Although, most of those our systems are able to identify within seconds or minutes of them signing up because the accounts just don't behave in the way a normal person would in using the service.

But this is certainly one of the highest priority issues we have. We see a large prevalence of it. Our systems I think at this point are pretty effective in fighting it but they're not perfect and there are still a few percent that get through--and--and it's a big issue and one we will continue working on.

KINZINGER: Thank you. I'd love to ask the rest of the others a question but I don't have time. So I yield back, Mr. Chairman. Thank you, for your attention.

DOYLE: I thank the gentleman. The Chair now recognizes Ms. Castor for five minutes.

CASTOR: Well, thank you, Mr. Chairman. Gentleman, since you were last here in front of the committee the illegal activities, the (INAUDIBLE) of unwitting Americans, rampant misinformation on your platforms have gotten worse. Part of the reason for this toxic stew is that you employ manipulative methods to keep people cemented to the platform often amplifying discord and it boosts your bottom line. You enjoy an outdated liability shield that incentivizes you to look the other way or take half measures while you make billions at the expense of our kids, our health, our truth. And now, we've seen the very foundation of our democracy.

I--I've been working over a year with advocates and other members with an update to the children's protections online. You all know that tracking and manipulation of children under age 13 is against the law. But Facebook, Google, YouTube and other platforms have broken that law or have found ways around it. Many have been sanctioned for knowingly and illegally harvesting personal information of children and profiting from--from it.

I have a question for each of you. It's a quick yes or no--did you all watch the social dilemma where former employees of yours or other Big Tech platforms say they do not allow their kids on social media--Mr. Zuckerberg?

ZUCKERBERG: Congresswoman, I haven't seen it but I'm obviously familiar with it.

CASTOR: Yes, sir. OK. Mr. Pichai, yes or no?

PICHAJ: Yes. I've seen the movie.

CASTOR: And--

DORSEY: No. No.

CASTOR: OK. Well, Mr. Zuckerberg, there is a good reason that they have the former execs say that. Are you aware of the 2019 journal of the American Medical Association Pediatric study that the risk of depression of adolescents rises with each daily hour spent on social media? And I'm not talking screen time. I'm not talking about Facetime or--or sending text messages to friends--are you aware of that research?

ZUCKERBERG: Congresswoman, I am not aware of that research.

CASTOR: All right, what about the 2019 HHS research that suicide rates among kids age 10 to 14 increased by 56 percent between 2007 and 2017 and tripled--tripled for kids between the age of 10 and 14--yes or no?

ZUCKERBERG: Congress--Congresswoman I'm aware of the--of the issues.

CASTOR: Yes. Certainly, you are also aware of the research that indicates a correlation between the rise in hospital admissions for self-harm and the prevalence of social media on phones--and the apps on platforms that are designed to be additive and keep kids hooked, yes? Well, how about you, Mr. Pichai, are you aware of the Journal of Pediatrics September 2020 study where they tested hundreds of apps used by children age five and under many of which were in the Google Play store's family section--the study found 67 percent of the apps tested show transmission of identifying info to third parties in violation of the COPA law--are you familiar?

PICHAJ: Extensively spent time on this area we introduced a curated set of apps for kids on the Play store. We give digital well-being tools so that people can take a break, set time patterns, can set time limits for children.

CASTOR: Let me ask you this then, Mr. Pichai--how much--how much are you making in advertising revenue from children under the age 13?

PICHAJ: Most of our products other than a specific product designed for kids and YouTube you know, most of our products are not eligible for children under the age of 13.

CASTOR: Yeah, so you're not going to provide that--Mr. Zuckerberg, how much advertising revenue does Facebook, do you make from behavioral surveillance advertising targeted towards kids under age 13?

ZUCKERBERG: Congresswoman, it should be none of it. We don't allow children under the age of 13 on any services that run advertising.

CASTOR: Oh, are you saying that there are no kids on Instagram under the age of 13 right now

ZUCKERBERG: Congresswoman, children under the age of 13 are not allowed on Instagram when we find out that they're there we remove them.

CASTOR: I think it's of course, every parent knows that there are--there are kids under the age of 13 on Instagram. And the problem is that you know it. And you know that the brain and social development of our kids is still evolving at a young age. There are reasons in the law that that we set that cut off at 13. Now, because these platforms have ignored it, they've profited off of it we are going to strengthen the law and I encourage all of my colleagues to join in this effort. I've heard a lot of bipartisan support here today.

We also need to hold the corporate executives accountable and give parents the tools that they need to--to take care and protect their kids. Thank you, Mr. Chairman. And I yield back.

DOYLE: Gentlelady's time is expired. Chair recognizes Mr. Johnson for five minutes.

JOHNSON: Thanks, Mr. Chairman. You know, over a decade ago Americans watched Facebook, Twitter and Google emerge from humble beginnings. We were curious to see how these new innovative companies would improve our lives. Results are in and they're deeply concerning.

We've seen a surge in cyber bullying, child porn, radical extremism, human trafficking, suicides and screen addiction all of which have been linked to the use of social media. Our nation's political discourse has never been uglier and we haven't been this divided since the civil war.

Yet, Big Tech marches on uninhibited. What's their newest target? Children under the age of 13. News outlets this week have reported that Facebook is planning to create an Instagram designed for children under the age of 13, we've talked about it here already today. Elementary and middle school students. By allowing Big Tech to operate under Section 230, as is, we'll be allowing these companies to get our children hooked on their destructive products for their own profit. Big Tech is essentially handing our children a lit cigarette and hoping they stay addicted for life.

You know, in 1994, Democratic Congressman Henry Waxman chaired a hearing with the CEOs of our nation's largest tobacco companies. During his opening statement he stated and I quote, "Sadly, this deadly habit begins with our kids. In many cases, they become hooked quickly and develop a lifelong addiction that is nearly impossible to break."

So, Mr. Zuckerberg and Mr. Dorsey, you profit from your company's hooking users to your platforms by capitalizing on their time. So yes or no, do you agree that you make money off of creating an addiction to your platforms--Mr. Zuckerberg?

ZUCKERBERG: Congressman, no. I don't agree with that.

JOHNSON: Thank you. Thank you.

ZUCKERBERG: What we do is--

JOHNSON: That's what I needed a yes or a no. Because you do. Mr. Dorsey?

DORSEY: No.

JOHNSON: OK. All right. Let me go on. Mr.--Chairman Waxman went on to say, and I quote, "For decades, the tobacco companies have been exempt from the standards of responsibility and accountability that apply to all other American corporations. Companies that sell aspirin, cars, and soda are all held to strict standards when they cause harm. And that we demand that when problems occur corporations and their senior executives be accountable to Congress and the public. This hearing marks the beginning of a new relationship between Congress and the tobacco companies." That is what Chairman Waxman said in 1994.

So for all three of you--Mr. Zuckerberg, Mr. Dorsey and Mr. Pichai, do you agree that the CEOs that as the CEOs of major tech companies you should be held accountable to Congress and the public? Mr. Zuckerberg.

ZUCKERBERG: Congressman, I think we are accountable to--to Congress and--and to the public.

[*]BILL JOHNSON: Should be held accountable.

ZUCKERBERG: I--I'm not sure I understand what you mean, but I think so.

BILL JOHNSON: It's a--question. Should you be held accountable to Congress and the public for the way you run your business?

ZUCKERBERG: Yes, and we are.

BILL JOHNSON: Okay. All right, thank you.

Mr. Dorsey?

DORSEY: Yes, accountable to the public.

BILL JOHNSON: Okay. Accountable, no. I said accountable to Congress and the public. We represent the public. So you agree?

DORSEY: Yes.

BILL JOHNSON: Okay, thank you.

Mr. Pichai?

PICHAJ: Yes, I'm here today because I'm accountable to Congress and members of the public.

BILL JOHNSON: Okay, great.

Well, gentlemen, let me tell you this. And--and I think I've heard it mentioned by several of my other colleagues. There's a lot of smugness among you. There's this air of untouchables in--in your responses to many of the tough questions that you're being asked.

So let me tell you all this. All of these concerns that Chairman Waxman stated in 1994 about big tobacco applied to my concerns about big tech today, about your companies. It is now public knowledge that former Facebook executives have admitted that they used the tobacco industry playbook for addictive products. And while this is not your first hearing in front of Congress, I can assure you that this hearing marks a new relationship between all of us here today. There will be accountability.

Mr. Chairman, I yield back.

DOYLE: I thank the gentleman. He yields back.

The chair now recognizes Mr. McNerney for five minutes.

MCNERNEY: Well, I thank the chair for organizing this hearing.

And I think the participants. This is a lot of work on your behalf and a long day for you. I appreciate that.

Are you all aware that your platforms are be myths and that the Americans are demanding that we step in and rein in your platforms? Both in terms of how you handle our data and how your platforms handle disinformation that causes real harm to Americans and to the democracy itself.

I understand the tension you have between maximizing your profits by engaging your platforms on the one hand, and but I need to--to address disinformation and the real harm it causes on the other hand. Your unwillingness to unambiguously commit to enforcing your own policies and removing the twelve most egregious spreaders of vaccine disinformation from your platforms gets right at what I'm concerned about. Disinformation is the strong driver for engagement, and consequently, you too often don't act, even though we know you have the resources to do that. There are real harms associated with this.

And my questions, I hope I don't appear to be rude, but when I ask for a yes or no question, I will insist on a yes or no answer.

Mr. Zuckerberg, yes or no, do you acknowledge that there is disinformation being spread on your platform?

ZUCKERBERG: Sorry, I was muted. Yes, there is, and we--we take steps to fight it.

MCNERNEY: Thank you.

Yes or no, do you agree that your company has profited from the spread of disinformation?

ZUCKERBERG: Congressman, I don't--I don't agree with that. People don't want to see disinformation on our services, and when we do, I think it hurts our long-term business.

MCNERNEY: You said--you said you don't agree with that. I appreciate your forthrightness--forthrightness on that.

But we all know this is happening. Profits are being generated from COVID-19 and vaccine disinformation, election disinformation, QAnon conspiracy theories, just to name a few things. And it's baffling that you have a negative answer to that question.

Approximately--well, let's move on to the next issue.

Mr. Zuckerberg, you talked a lot about relying on third-party fact-checkers to combat the spread of disinformation, but you tell us very little about the process. I wrote you a letter nearly two years ago asking about it, and you failed to answer my question. I asked this question again. When an executive from your company testified last year, and she failed to answer it. I'd like to get an answer today.

On average, from the time content is posted to Facebook's platform, how long does it take Facebook to flag suspicious content to third-party fact checkers--for third-party fact-checkers to review the content and for Facebook to take remedial action after this review is completed? How long does this entire process take? I'm just looking for a quick number.

ZUCKERBERG: Congressman, it can vary. If an AI system identifies something immediately, it can be within seconds. If we have to wait for people to report it to us and have human review, it can take hours or days. The fact-checkers take as much time as they need to review things, but as soon as we get an answer back from them, we should operationalize that and attach a label if the content is rated false and reduce the--.

MCNERNEY: Okay.

I understand what you're saying. But what I do know is that this process isn't happening quickly enough. And I'm very concerned that you aren't motivated to speed things up because most problematic content is what gets the most views. And longer the content stays up, the more help--the more this helps maximize your bottom line and the more harm that it can cause.

It's clear that you aren't going to make these changes on your own.

This is a question for all of the participants' panelists. Would you oppose legislation that prohibits placing ads next to what you know to be or should know to be false or misleading information, including ads that are placed in videos, promoted content, and ads that are placed above, below or on the side of a piece of content?

Mr. Zuckerberg, would you answer with a yes or no first, please?

ZUCKERBERG: Congressman, that--that's very nuanced. I think the--the question is to determine whether something is misinformation is a--is a process that I think would need to be spelled out well in a--in a law like that.

MCNERNEY: Well, okay. I appreciate that.

Mr. Dorsey?

DORSEY: Yes, I would--until we see the actual requirements and what the ramifications are. We need to understand that.

MCNERNEY: Okay.

Mr. Pichai, would you oppose the prohibition like this?

PICHAJ: The principle makes sense. In fact, advertisers don't want anywhere or near to be content like that. And so, we will already have incentives. You can imagine reputable advertisers like consumer products advertisers do not want any ads to appear next to information that could turn off their consumer. So we have natural incentives to do the right thing here.

MCNERNEY: You all say you want a safe and open platform for everyone. You say it's not in your company's interest to have disinformation on your platform. So you shouldn't oppose efforts that prevent--that would prevent harming American people.

I yield back.

DOYLE: The gentleman's time has expired. The gentleman yields back.

The chair now recognizes Mr. Long for five minutes.

LONG: Thank you, Mr. Chairman.

Mr. Pichai, I'm going to ask you a yes or no question and just tell me the difference in these two words. Yes and no.

PICHAJ: Yes.

LONG: Mr. Zuckerberg, same question for you. Do you know the difference in yes or no?

ZUCKERBERG: Yes, Congressman.

LONG: And Mr. Dorsey, same question for you. Do you know the difference in the two words, yes or no?

DORSEY: Yes, sir.

LONG: I'm sorry.

DORSEY: Yes, I do know the difference.

LONG: Okay, thank you.

I just--I won a steak dinner there from one hour--my colleagues. They didn't think I could get you all to answer. All three of you can answer yes or no questions. I did it.

Mr. Zuckerberg, let me ask you. How do you ascertain if a user is under 13 years old?

ZUCKERBERG: Congressman, on services like Facebook, we have people put in--a birthday when they--when they register.

LONG: That's handy.

So a thirteen-year-old would never--I mean, an eleven-year-old would never put in the wrong birthday by two years and say they were thirteen. Is that kind of your policy?

ZUCKERBERG: Congressman, it's more nuanced than that. But I think you're getting at a real point, which is that people lie. And we--we have additional systems that try to determine what someone's age might be. So if we detect that someone might be under the age of thirteen, even if they lied, we kick them off.

But this is part of the reason why we're exploring having a service for--for Instagram that--that allows under-thirteens on because we worry that kids may find ways to try to lie and evade some of our systems. But if we create a safe system that has appropriate parent controls, then we might be able to get people into using that instead. We're still early in figuring this out, but--but that's a big part of the--the theory. And what we're hoping to do here.

LONG: And currently, they're not allowed to use Instagram, correct?

ZUCKERBERG: That's correct. Our policies do not allow people under the age of thirteen to use it.

LONG: I'm from Missouri, the show me state, and just to say that no one under thirteen could get on to me, doesn't pass the Missouri smell test of show me, so.

Sticking with you, Mr. Zuckerberg. You created the Facebook Oversight Board as a way to help hold Facebook accountable. They are currently looking at Facebook's decision to remove President Trump's Facebook account. If the Oversight Board determines that Facebook should have left President Trump's account up, what will you do?

ZUCKERBERG: Congressman, we will respect the decision of the Oversight Board. And--and if they tell us that former president Trump's account should be reinstated then--then we will honor that.

LONG: I don't know why people call Attorney General Ashcroft, Attorney General, but when they speak of President Trump they just call him former president. But I guess I'll leave that for another day. Sticking with you again, Mr. Zuckerberg. It's my understanding is that Facebook Oversight Board is comprised of members from all over the world. As you're well aware, the United States has the strictest protections on free speech than any other country.

Since the decisions of the board are being made by a panel rather than the U.S. court of law, how can you assure members of this committee and the American people that the oversight board will uphold free speech and make their decisions based on American laws and principle?

ZUCKERBERG: Congressman, the--the members of the Oversight Board were selected because of their views on free expression and strong support of it. That's why we created the oversight board, to help us defend these--these principles. And--and to help us balance the different aspects of human rights including free expression. But each of the people on the oversight board was selected because of a strong commitment to free expression.

And I think the decisions that the oversight board has made so far reflect that.

LONG: Okay. Let me move on to Mr. Dorsey. Mr. Dorsey, I know you're from the show me state also. Have you been vaccinated against COVID-19?

DORSEY: Not yet.

LONG: Mr. Pichai, have you been vaccinated against COVID-19?

PICHAJ: Sorry, I'm--I missed the question, Congressman.

LONG: Have--have you--I know, I bore a lot of people. Have you been vaccinated against COVID-19?

PICHAJ: Congressman, I was very fortunate to have received it last week.

LONG: So you have one shot, you have another one to go? Or is it just Johnson & Johnson where you just need one?

PICHAJ: I--I still have one more shot to go.

LONG: And Mr. Zuckerberg, same question. Have you been vaccinated against COVID-19?

ZUCKERBERG: I have not yet but hope to as soon as possible.

LONG: Okay. It's not a personal preference not to get vaccinated, you just haven't got to your age group or?

ZUCKERBERG: That's correct.

LONG: Okay. Thank you. And I just cannot believe Robert Kennedy, Jr. is out there with his anti-vax stuff and it's allowed to stay up on Twitter. With that, I yield back.

DOYLE: Gentleman yields back. Let's see, who's next. I don't see a name. Can staff show us who's next up? Mr. Welch, you're recognized for five minutes.

WELCH: And thank you, Mr. Chairman. What we're hearing from both sides of the aisle are enormous concerns about some of the consequences of the development of social media. The algorithmic amplification of disinformation, election interference, privacy issues. The destruction of local news, and also some competition issues.

And I have listened carefully and each of the executives has said that your companies are attempting to face these issues. But a concern I have is whether when the public interest is so affected by these decisions and by these developments. Ultimately should these decisions be made by private executives who are accountable to shareholders or should they be made by elected representatives accountable to voters?

So I--I really have two questions that I'd like each of you starting with Mr. Zuckerberg and then Mr. Pichai and then Mr. Dorsey to address. First, do you agree that many of these decisions that are about matters that so profoundly affect the public interest, should they be made exclusively by private actors like yourselves who have responsibilities for these major enterprises?

And secondly as a way forward to help us resolve these issues or work with them, will you support the creation by Congress of a public agency, one like the Federal Trade Commission or the Securities and Exchange Commission, one that had staff that's expert in policy and technology. It has rulemaking and enforcement authority to be an ongoing representative of the public to address these emerging issues.

Mr. Zuckerberg.

ZUCKERBERG: Congressman, I--I agree with what you're saying and I--I've said a number of times that I think that private companies should not be making so many decisions alone that have to balance these complicated social and public equities. And I think that the solution that you're talking about could be very effective and positive for helping out. Because what we've seen in different countries is--around the world--is the--there are lots of different public equities at stake here, free expression, safety, privacy, competition.

And these things trade off against each other, and I think a lot of these questions and--and the reason why people get upset at the companies, I don't think it's necessarily because the companies are negligent. I think it's because these are complex tradeoffs between these different equities. And if you set up--

WELCH: --Pardon my interruption. But I wanna go to Mr. Pichai. But thank you, Mr. Zuckerberg.

PICHAU: Congressman, if your question is--I just wanna make sure--are you asking about whether there should be another agency I defer to Congress on that. We are definitely subject to a variety of statutes and oversight by agencies like FTC. We have constant degree--agreements with FCC. And we engaged with these agencies regularly.

WELCH: But do you believe that it should be up to the public as opposed to private interests to be making decisions about these public effects?

PICHAU: We--we definitely think areas where there could be clear legislation informed by the public, I think that definitely is a better approach. I would say the nature of content is so fast changing and so dynamic, you know, we spend a lot of area hiring experts, consult with third parties, and that expertise is needed I think based on the nature of the (INAUDIBLE)--

WELCH: --Right. And that's the--that's the problem we have in Congress. Because an issue pops up and there's not a way we can keep up when you all can barely keep up with it yourself. Mr. Dorsey, your view on those two questions, please.

DORSEY: I--I--I--yes, I don't think the decision should be made by private companies or the government. Which is why we're suggesting a protocol approach to help the people make the decisions themselves, have more control themselves.

WELCH: So does that mean that the creation of an agency that would be intended to address many of these tech issues that are emerging is something you'd oppose or not?

DORSEY: Well, it--always have an open mind. I'd want to see the details of--of what--what that means and--and how it--how it works in practice.

WELCH: Well, you--of course. But the heart of it is creating an entity that has to address these questions of algorithmic transparency, of algorithmic amplification of hate speech, of disinformation, of competition. And to have an agency that's dedicated to that much like the Security Exchange Commission was designed to stop the rampant abuse on Wall Street in the thirties.

A public sector entity that is doing this, not just leaving it to private companies.

DORSEY: Yeah. I--I--

WELCH: --Do you agree or not?

DORSEY: I do think there should be more regulation around the primitives of AI. But we focus a lot of our conversations right now on the outcomes of it. I don't think we're looking enough at the primitives.

WELCH: Thank you. I yield back.

DOYLE: Gentleman yields back. Chair recognizes Mr. Bucshon for five minutes.

BUCSHON: Thank you, Mr. Chairman. And first of all I wanna thank the witnesses for being here today. It's gonna be a long day and I appreciate your--your testimony and your answering questions. I--I do think it's important to understand history--excuse me--when you look at these situations. And you know, when it comes to the political side, when Thomas Jefferson wanted to get out an anti-Adams message even though he was his own vice president, he started his own newspaper because it was pretty clear that the newspapers that were being published weren't gonna change their--their view because there was no competitive reason to do that.

And I think we're looking at potentially a similar situation here. A com--without competition things don't change. I mean, it'd be interesting to know the conversations with John D. Rockefeller in the early 1900s, prior to the breakup of Standard Oil in 1911, and then of course AT&T in 1982. So I, you know, I understand that these are businesses. They're publicly held companies. I respect that. I understand that. I'm--I'm a capitalist.

That said, there is--these are a little different I think because there's some social responsibility here and I appreciate your answers that your companies are doing what you believe are necessary. But--so I wanna ask--I'm gonna take this--the anti-trust angle here and Mr. Pichai, what do you think--what do--what's the situation when you have Google-- 92 percent of the searches are Google. You basically can't get on the internet without some sort of Google service.

What do you think--what do you think is gonna happen? What do, you know, what do you think we should do about that?

PICHAU: Congressman, I'm--me--we definitely are engaged with conversations as well as

[*]PICHAU: lawsuits in certain cases. We understand there will be scrutiny, we are a popular general purpose search engine but we compete vigorously in many of the markets we operate in. For example, majority of revenue comes from product searches and one in two product searches originate with Amazon today in the U.S. so we definitely see a lot of competition by category. There are many areas as a company, we are an emerging player be making phones or when we are trying to provide enterprise software we compete with other larger players as well.

And, if you look at last year and look at all the new entrants in the market new (INAUDIBLE) public and emerged strongly you know in--in tech shows that the market is vibrant and dynamic. As Google, we have invested in many startups. Googlers started over--former Google employees have started over 2000 companies in the past 15 years. And so, you know, I see highly dynamic, vibrant, competitive tech sector. And we are committed to doing our part.

BUCHSON: OK. Fair enough. Mr. Zuckerberg, do you have some comments on that subject?

ZUCKERBERG: Congressman, I would echo Sundar's comments. I think that this is a highly competitive market. I mean, if this is a meeting about social media not only do you have the different companies that are here today that all offer very big services that compete with each other but you have new entrants that are growing very quickly like TikTok, which is--is reaching a scale of--of hundreds of millions or billions of people around the world. And I think it is growing faster than any of our services of--of the companies that are--that are up here today and certainly competitive with us and that is just naming a few. Right, obviously there's--there's Snapchat and a bunch of other services as well.

So it's a very competitive marketplace.

BUCHSON: And do you think, and I ask you this, Mr. Zuckerberg--you I think you've commented that some of the privacy things that maybe the Europeans did would kind of solidify your--your dominance as a company. So what should we do in--in the United States on--on this because it's a different subject but similar to the to not do something that would stymie innovation competition and further, in my view, further create a monopolistic or at least a perceived monopolistic environment?

ZUCKERBERG: Well, Congressman, I do think that the U.S. should have federal privacy legislation because I--I think we need a national standard and I think having a standard that is across the country as harmonized with standards in other places would actually create clearer expectations of industry and make it better for everyone. But I think the point that you are making is a really important one which is if we ask companies to lock down data then that to some degree can be at odds with asking them to open up data to enable whether it's academic research or competition. So I think that when we're writing this privacy legislation we just should be aware of the--the interaction between our principles on privacy and our principles on competition. And that's why, I think a more holistic view like what Congressman Welch was just proposing I think is--is perhaps a--a good way to go about this.

BUCHSON: OK. Quickly, Mr. Dorsey, you have any comments on that?

DORSEY: One--one of the reasons we're suggesting more of a protocol approach is to enable as many new entrants as possible. We--we want to be a client on that.

BUCHSON: My time has expired. With that, I yield back.

DOYLE: Chair recognizes Ms. Clarke for five minutes.

CLARKE: Thank you, Mr. Chairman I thank you the--the chairs and the ranking members for today's hearing. I also thank our witnesses for appearing.

In January I called for a public comment for the discussion draft of my bill. The Civil Rights Modernization Act of 2021, a narrowly focused proposal to protect historically marginalized communities from the harms of targeted advertising practices. These harms can and have infringed on the civil rights of protected classes. And I'm proud to formally introduce this bill next week to diminish inequities in the digital world. For--for time's sake, I ask our witnesses to please answer the questions as succinctly as possible.

The first question goes to Mr. Zuckerberg. Facebook currently provides their advertisers with insight on how to get their ads in front of people who are most likely to find their ads relevant by utilizing tools to use criteria like consumer's personal interests, demography, to finetune the targeting. This is often used code that target or avoid specific races or other protected classes of people. Let me add that I am aware of the updates to your special ad audience. However, why does Facebook continue to allow for discrimination in the placement of advertisements that can violate civil rights laws?

ZUCKERBERG: Congresswoman, we've taken a number of steps to eliminate ways that people can target different groups based on racial affinity and--and different ways that they might discriminate cause this--this is a very important area. And we have active conversations going on with civil rights experts as to the--the best ways to continue improving these systems and will continue doing that.

CLARKE: Mr. Dorsey, Twitter allows advertisers to use demographic targeting to reach people based on location, language, device, age and gender. In July, your company made changes to your ad targeting policy to advise advertisers to quote, "not wrongfully discriminate against legally protected categories of users," end quote. What did Twitter mean by the phrase, "wrongfully discriminate"? Are some kinds of discriminatory advertising permitted on Twitter? If so, would you please explain?

DORSEY: No. None at all.

CLARKE: I'm sorry I--I didn't get that answer.

DORSEY: No. None at all.

CLARKE: OK. So can you explain what--what you meant by a won't wrongfully discriminate?

DORSEY: We--we mean that we you shouldn't just use our app systems to discriminate.

CLARKE: Oh, OK. Mr. Pichai, Google has recently announced a new approach in their targeting system called FLOC or federal learning of cohorts. Excuse me, federated learning of cohorts--to allow an--an ad targeting to groups of people who have similar characteristics. The new system will utilize machine learning to create these cohorts for the consumer's visits to websites. Given the potentially biased and disparate impact of learned--machine learning algorithms how has Google addressed the potential discriminatory impact of this new FLOC system?

PICHAJ: Congresswoman, it's an important area--we recently announced a joint collaboration with HUD to ban ads that would target age, gender, family status, Zip Code in addition to race, which we have long disallowed. So we'll bring similar prohibitions particularly when we are using machine learning. And by the way FLOC although we haven't implemented it yet--we will be publishing more technical proposals on it. And we will they will be held to our AI principles which prohibit you know, discrimination based on sensitive categories including race and we--we will be happy to consult and explain our work there.

CLARKE: I appreciate that. Gentleman, I just want you to be aware that the longer we delay in this the more that these systems that you have created bake discrimination into these algorithms. I think that is critical that you get in there and that you do what is in the best interest of the public of the United States of America and un--undo a lot of the harm that has been created with the bias that has been baked into your systems.

With that, Mr. Chairman, I yield back 23 seconds and I thank you for this opportunity.

DOYLE: And it hank the gentlelady for that. The Chair now recognizes Mr. Walberg for five minutes.

WALBERG: Thank you, Mr. Chair and thanks to the panel for being here. You know, what I've--what I've listened to so far today I'd have to say based upon what many of us in Congress say about the best legislation when both sides don't like it it's probably--probably good. And you certainly hit that today. I think from both sides you--you have been attacked for various reasons.

But you know, I have to say the--the platforms you have developed are amazing and they have huge potential. And they indeed have enabled us to go directions information, communications, relationships that can be very positive and are amazing what--what's been accomplished. I think that will get down to how that is controlled and who controls it. Going back to our foundations as our country was our second president, John Adams, who said that our Constitution was meant for a moral and religious and is solely inadequate for any other.

I think we're seeing a lot of the problems that you're frustrated with as a result of parents and families, churches, schools that aren't taking the primary responsibility. I get that. So, it comes down to the choice that's left for the people is really between conscience and the constable. We're either going to have a conscience that self-controls, and as you have said Mr. Zuckerberg--I--you know, in fact what you said, I wouldn't mind my three and five-year-old granddaughters coming to your house. I'm not asking for the invitation, but I think they'd be safe there relative to the online capabilities, from what you've said. But that's conscience versus constable.

But what I've hear--heard today is that there will be some constable, and I'm not sure that we'll have success in moving forward. So, I guess, Mr. Chairman, unfortunately we've been here before. We been here many times.

A few years ago when Mr. Zuckerberg was here before this committee, I held up a Facebook post by a state senator in Michigan that--whose post was simply announcing his candidacy as a Republican for elected office, and yet it was censored as shocking and disrespectful or sensational in content. Just a few months ago, I posted my resolution that would add teachers to the vaccine priority list on Twitter, and it was labeled as "sensitive content" and encouraged to be changed.

Well, hiding behind Section 230, all of you have denied that there is any bias or any inequitable handling of content on your platforms, and yet Pew Research Center found that--and this is where I have my problem, not so much with the platform or even the extent of what's on the platform. But they found that 72 percent of the public thinks it's likely that social media platforms actively censor political views that Big Tech companies find objectionable. Further, and I quote, "By a 4 to 1 margin, respondents were more likely to say Big Tech supports the views of liberals over conservatives and vice versa," probably equaled only by higher education. That was my--my statement.

And yet every time this happens, you fall back on blaming glitches in the algorithms. It was former--Greg Copolla, formal Google insider, who said--before he was suspended by Google, he said algorithms don't write themselves. We write them to do what we want them to do. That's my concern. Whether it's censoring pro--pro-life groups like Life Action or pro-Second Amendment groups like the Well Armed Women, your platforms continually shut down law-abiding citizens and constitutional discussions and commerce that don't align with Big Tech views and the worldview. And this includes the First and Second Amendments, that causes me to be concerned that you don't share the same freedom and constitutional concerns.

It's not often I find myself agreeing with Bernie Sanders. But in an interview earlier this week, and I quote, he said, "If you're asking me do I feel particularly comfortable that the president of the United States should not express his views on Twitter, I don't feel comfortable about that." He went on to say, "Because yesterday was Donald Trump who was blamed and tomorrow it could be somebody else."

Mr. Zuckerberg and Mr. Dorsey, do you think the law should allow you to be the arbiters of truth as they have under Section 230? Mr. Zuckerberg first.

ZUCKERBERG: Congressman, I--I--I think that it is good to have a law that allows platforms to moderate content. But I--I--as I've said today, I think that there--that we do benefit from--for more transparency and accountability.

WALBERG: Mr. Dorsey?

DORSEY: I don't think we should be the arbiters of truth, and I don't think the government should be either.

DOYLE: The gentleman's time is expired.

WALBERG: I agree. I yield back.

DOYLE: The chair now recognizes Mr. Cardenas for five minutes.

CARDENAS: Thank you very much, Mr. Chairman and ranking members for having this important hearing. I'd like to submit to the record a National Hispanic Media Coalition letter against Spanish-language disinformation and social media. And if we could submit that for the record I'd appreciate that.

And also, my first question is to you, Mr. Zuckerberg. In 2020, Facebook brought in approximately \$86 million of revenue in 2020. Is that about right, give or take?

ZUCKERBERG: Congressman, I think that's about right.

CARDENAS: Okay, thank you. Good. How much of that revenue did Facebook invest in identifying misinformation, disinformation in a portion of your business?

ZUCKERBERG: Congressman, I don't know the exact answer, but we invested billions of dollars in--in our integrity programs, including having more than 1000 engineers working on this and 35,000 people doing content review across the company.

CARDENAS: Okay. And how many people do you have--full-time equivalents in your company overall?

ZUCKERBERG: Congressman, I don't know the exact number, but I think, you know, it's around 60,000.

CARDENAS: Okay. So, you're saying over half of the people in your company are doing the portion of content review, etc., which is the main subject we seem to be talking about today.

ZUCKERBERG: No, Congressman, because you--you asked about full-time employees, and--and some of the content to reviewers are contractors.

CARDENAS: Oh, okay. All right. Well, there seems to be a disparity between the different languages that are used on your platform in America. And as--for example, there was a study published in April by Avast, and over 100 items of miss--of misinformation on Facebook and six different languages was found, but 70 percent of the Spanish-language content analyzed had not been labeled by Facebook as compared to 30 percent of the English-language misinformation that had not been labeled. So, there seems to be a disparity there.

What kind of investment is Facebook making on the different languages to make sure that we have more of a--of inaccuracy of applying those--the disinformation and misinformation?

ZUCKERBERG: Congressman, thanks. We--we have a--an international fact-checking program where we work with fact-checkers and more than 80 countries and in a bunch of different languages. In the U.S. specifically, we--we have Spanish-speaking fact-checkers as well as English-speaking fact-checkers, so that's on the misinformation side. But also, when we create resources with authoritative information, whether it's on--around COVID information or election information, we translate those hubs so that way they can be available in both English and Spanish. And we make it so people can see the content in whatever language they prefer.

CARDENAS: Thank you.

ZUCKERBERG: Thank you.

CARDENAS: So, basically you're saying it's extensive.

ZUCKERBERG: Congressman, this is certainly something that we invest a lot in, and it will be something that we continue to invest more in.

CARDENAS: Okay. I--I like the last portion. I--I do believe and would love to see you invest more.

I--my 70-plus-year-old mother-in-law, who is primarily a Spanish speaker, commented to me the other day that her friends, who communicate mainly in Spanish, and they do use the internet, they do use some of your platforms, gentlemen, that they were worried about the vaccine and that somebody's going to put a chip in their arm. For God's sakes, I mean, that to me just was unbelievable, that they would comment on that.

But they got most of that information on the internet, on--on various platforms. Clearly, Spanish-language disinformation is an issue, and I'd like to make sure that we see all of your platforms address these issues not only in English but in all languages. I think it's important for us to understand that--that a lot of hate is being spewed on the internet, and a lot of it is coming through many of your platforms.

For example, there are 23 people dead in El Paso because somebody filled this person's head with a lot of--a lot of hateful nonsense, and he drove to specifically kill Mexicans along the--the Texas-Mexican border. Eight people are dead in Atlanta because of anti-Asian hatred and misinformation has been permitted to spread and allowed on--on these platforms unchecked--pretty much unchecked.

The spread of hatred and incitement to violence on platforms is a deadly problem in America, and I—we—we need to see that it stops. Mr. Zuckerberg, do you believe that you've done enough to combat these kinds of issues?

ZUCKERBERG: Congressman, I—I believe that our systems and—that we've done more than—that basically any other company, but I think that there is still a problem and there's still more that needs to be done.

CARDENAS: Okay. It's good you to—you'd like to do more. Thank you. I only have 15 seconds, I'm going—this question to all three of you. Do you think that each one of your organizations should have an executive-level individual in charge of this department reporting directly to the CEO? Do you think you agree that that should be the case? Mr. Zuckerberg?

ZUCKERBERG: Congressman, we—we have an executive level person who's in charge of the—the integrity team that I talked about. He's on my management team.

CARDENAS: He reports directly to you?

ZUCKERBERG: Congressman, he—he does not. I only have a few direct reports. A lot of the people on the management team report to them.

CARDENAS: Thank you. To the other two witnesses very quickly?

PICHAU: Congressman, we have senior executives, including someone who reports directly to me, who oversees trust and safety across all these areas.

CARDENAS: Thank you. Mr. Dorsey?

DORSEY: We do.

CARDENAS: Thank you so much and I yield back the time.

DOYLE: The gentlemen's time is expired. The Chair now recognizes Mr. Carter for five minutes.

CARTER: Thank you, Mr. Chairman, and thank all of you for being here. Mr. Zuckerberg, I'd like to start with you and I wanted to ask you you're aware as all of us are of the—of the disaster that we have at the southern border. (INAUDIBLE) indicate that human smugglers have been using social media, including Facebook, WhatsApp, and Instagram to coordinate their operations in transporting illegal immigrants into the United States.

Things like—like what to say to authorities, transportation tips, and other forms of information that are being traded on your platform to evade authorities and contribute to the crisis, this disaster at the border. Mr. Zuckerberg, do you feel complicit in any way that your platform is—is assisting in this disaster?

ZUCKERBERG: Congressman, first let me say that what's happening at the border is—is a--

CARTER: --I'm—I'm not—we know what's happening at the border. I'm asking you specifically about your platform. Do you feel complicit in what your platform is doing to assist in this disaster?

ZUCKERBERG: Congressman, we—we're—we're—we have policies and we're working to—to fight this content. We have policies against scams in—in pages, groups, and events like the content that you're talking about. We're also seeing the State Department use our platform to share factual information with people about (INAUDIBLE)--

CARTER: --But we're talking about—the facts is I'm talking about—I'm talking about coyotes who are using your platform to spread this kind of information to assist in this illegal activity that is resulting in—in—in horrible conditions for these people who are trying to come across that border.

ZUCKERBERG: Congressman, that's against our policies and we're taking a lot of steps to stop it. And—and again, I mean, let me just say that I think that the situation at the border is really serious and—and we're taking it very seriously.

CARTER: Well, and I hope you'll look into this. These reports that your platform is being used by these traffickers, this is something we need your help with. I hope you feel a sense of responsibility, sir, to help us with this. Because we certainly need it.

Let me ask you something. You've dedicated a—a lot of your written re—testimony to election issues and even today during this—during this hearing you've been very public in pushing back about the election claims in November. Yet, when Facebook has been essentially silent on the attempted theft of the certified election in Iowa

of Representative Miller-Meeks, why is that? Why are you silent on that yet you're not silent on other elections?

ZUCKERBERG: Congressman, I think what we saw leading up to January 6th was unprecedented in--in American history where you had a sitting president trying to undermine the peaceful transfer of--of power--

CARTER: --You confirming which one is important and which one is not. This seat to these people who elected this duly certified representative, this is the most important thing to them as well.

ZUCKERBERG: Congressman, I think part of what made the January 6th events extraordinary was not just the--that the--the election was contested but that you--you've got folks that--

CARTER: --What? Okay, then let me ask you this. What is it that makes this particular issue irrelevant? That you're not even covering it.

ZUCKERBERG: Congressman, I didn't say that it's irrelevant. But it--it--but it--on January 6th we had insurrectionists storm the Capitol leading to the death of multiple people--

CARTER: --I--I--Mis--Mr. Zuckerberg I'm--I'm aware of that. I was there. I understand what happened. But again, will you commit to treating this as a serious election concern?

ZUCKERBERG: Alright. Congressman--

CARTER: --What's going (INAUDIBLE)?

ZUCKERBERG: Congressman, we--we--I--I will commit to--to--to that and we apply our policies to--to all situations. And--and I think that this is different from what happened on January 6th but we apply our--our policies equally in these cases.

CARTER: Mr.--Mr. Dorsey, you too have been very silent on this issue on your platform. Will you commit to may--to treating this as a serious concern, the attempted theft of the certified seat in Iowa?

DORSEY: Yes, we're looking for all opportunities to minimize anything that takes away from the integrity of elections.

CARTER: Okay. Mr.--Mr. Dorsey while I've got you, let me ask you. You've--you've started a new program. It's called the Birdwatch. And it allows people to identify information in tweets that--that they believe is misleading and they write notes to provide context in an effort to stop misleading information from spreading.

Have you seen whi--we've seen mobs of Twitter users cancel others even when the information they share is accurate. Why do you think Birdwatch is gonna work given the culture that you created on your platform?

DORSEY: Well, it's an experiment. I mean, we're--we're--we wanted to experiment with more a crowd-source approach than us going around and--and doing all this work.

CARTER: Don't you think that's kind of a dangerous experiment when you're taking off truthful information?

DORSEY: No, it's an alternative. And I think--

CARTER: --An alternative?

DORSEY: I think we need to experiment as much as possible to get to the right answers. I think it stinks--

CARTER: --Okay, well that's--that's fine as long as you're not the one being experiment on, as long as you're not the one that the information--

DORSEY: --We're not (INAUDIBLE)--

CARTER: --The truthful information (INAUDIBLE)--

DOYLE: --The gentleman's time--

DORSEY: --Can use it--

DOYLE: --The gentleman's time is expired--

CARTER: --Yield back--

DOYLE: --The Chair announces that we are going to take a recess now for 15 minutes. So the committee will stand in recess until 3:18 and then we'll come back promptly. I call the committee in recess.

(RECESS)

DOYLE: Ask all members and witnesses to come back online. OK. We'll get started. The Chair recognizes. Ms. Dingell, for five minutes

DINGELL: Thank you, Mr. Chairman. Thanks for having this hearing and to everyone for testifying today. We can all agree that social media companies have a responsibility to reduce and eliminate the effect of disinformation on their platforms. Mr. Zuckerberg, in the fall of 2020 you made numerous assurances to Congress that you had a handle on militia and conspiracy networks. We know however, that Facebook private groups and the algorithms that recommend them have assisted in radicalizing users and facilitated terrorism, violence and extremism against individuals including the governor of my state in Michigan.

Racial and ethnic minorities, including Muslims and recently, Asian Americans are facing growing racist hate online and violence offline. Last year, I sent you multiple letters about these issues so I know you're aware of them.

In October of 2020 Facebook temporarily decided to stop recommending political and civic groups on its platforms. Change has now made permanent. But to be honest, despite what you did in October, we had an insurrection that stormed the Capitol on January 6th.

I seriously question Facebook's commitment to actually stopping extremism. In a recent investigative report a former Facebook AI researcher said he and his team conducted study after study confirming the same basic idea--models that maximize engagement increase polarization. And you, yourself have said the more likely content is to violate Facebook community standards the more engagement it generally receives. Engagement is the key to Facebook's growth and success. And the stock market has rewarded you for it, even as you been criticized for promoting extremism and racist content including in a 2020 Facebook civil rights audit.

The two seem to go hand in hand as Facebook also was the most cited social media site in charging documents that the Justice Department filed against the Capitol Hill insurrectionists. Mr. Zuckerberg, do you still maintain that the more likely user content is to violate Facebook community standards the more engagement it will receive, yes or no?

ZUCKERBERG: Congresswoman, thanks for--for raising this because I think that there's been a bunch of--of inaccurate things about this shared today. There seems to be a belief--

DINGELL: Can I (INAUDIBLE) yes or no?

ZUCKERBERG: Sorry this--this is a--a nuanced topic. So if--if you--if--if you're OK with it I'd like to explain what--what--

DINGELL: Sure. But I'll give it seconds since I (INAUDIBLE) victim of this hate.

ZUCKERBERG: People don't want to see misinformation or divisive content on our services. People don't want to see clickbait and things like that. While it may be true that people may be more likely to click on it in the short term it is not good for our business or our product or our community for our content to be there. It's not what people want and we run the company for the long-term with--with a view towards 10 or 20 years from now and I--I think that we are highly aligned with our community and--in trying to not show people the content that's not going to be meaningful to them.

DINGELL: OK. Mr. Zuckerberg I'm going to--I only have two minutes left. Do you still agree with the statement in Facebook's most recent filing that the first risk related to your product--product offerings is our ability to add and retain users and maintain levels of user engagement with our products--just a yes or no, please?

ZUCKERBERG: Congresswoman, I think that that's generally right I mean for any product ability to--to build something that people like and use is--is something that--that is a risk if we can't do that.

DINGELL: OK. So do you still agree with the statement of your CFO on a recent earnings call that the changes to group recommendations so far wouldn't affect your engagement yes or no?

ZUCKERBERG: Congresswoman there are so many different parts of--of the service that I think it's probably right that not--not--not recommending political or civic groups probably isn't going to meaningfully decrease engagement. But we have taken a lot of other steps including you know, reducing viral videos by about 50 million hours of watching a day--which have had meaningful impact on engagement but we--we do that because we--it helps make the service better and helps people to like it more which I think will be better for both the community and our business over the long-term.

DINGELL: OK. Mr. Zuckerberg I'm sorry to have to do this in five minutes--but given your promises in the fall the events that transpired on January 6, in your true incentives you yourselves admit I find it really difficult to take some of these assurances you are trying to give us today seriously. I think that regulators and independent researchers should have access to Facebook and other large social media platforms recommendations, algorithms--not just for groups but for any relevant feature that can be exploited or exploit private user data collected by the company to support extremism. And I support legislation to do so. Mr. Zuckerberg, given your inability to manage your algorithms or your unwillingness to--to reduce controversial content are you opposed to a law enabling regulators to access social media algorithms or other information technology that result in a promotion of harmful disinformation and extremist content?

ZUCKERBERG: Well, Congresswoman while I don't necessarily agree with your characterization I do think that giving more transparency to the systems is an important thing. We have people working on figuring out how to do this. One of the nuances where in complexity is that it is hard to separate out the algorithms versus people's data which--which kind of goes into that to make decisions and the data is private so it's tough to make that public and transparent. But I do think that this is an important area of study on how to audit and--and make algorithms more transparent.

DOYLE: OK. The gentlelady's time is expired. The Chair recognizes Mr. Duncan for five minutes.

DUNCAN: Thank you, Mr. Chairman. Let me first say that democrats are repeating disinformation about the motives of the murder in Atlanta during a hearing on disinformation is irony at its worst. The murderer admitted that he was a sex addict. The problem was addiction, mental illness. While my thoughts and prayers go out to the families who are impacted by this hideous crime, it was not a hate crime and to say so is misinformation.

Mr. Dorsey, is it OK for a white male to tweet a picture of a KKK clansmen hood to a black woman?

DORSEY: No that would go against our hateful conduct policy.

DUNCAN: Just this week, black conservative commentator Candice Owens was sent a tweet from a white liberal depicting a KKK hood and your support center said that that racist harassment--harassment of a conservative didn't violate your terms of service. What do you have to say about that?

DORSEY: We have we--we removed that tweet.

DUNCAN: OK. Thank you for doing that. Also this week, Syrian refugee Ahmad al Alawi Aleesa, a Biden-supporting Muslim, allegedly murdered 10 people at a grocery store in Boulder, Colorado. Your support center told Newsweek that referring to this gentleman as a white Christian terrorist wasn't in violation of your misinformation policy. What do you have to say about that?

DORSEY: I don't know that case but we can follow-up with you on it.

DUNCAN: Thank you. Your promises and from the last hearing that you'll work on this or make it better ring completely hollow sometimes. So I ask that you do. You've censored and taken down accounts of conservatives, Christian and even prolife groups. At the same time liberals, tyrants and terrorists continue to have unfettered access on Twitter. You are able to take down the account of a sitting United States President, while he was still president. But you continue to allow state sponsors of terror to use Twitter as a platform including the Ayatollah Khamenei, Javad Zarif of Iran or even Bashar Assad of Syria.

You act like judge and jury and continue to hide behind the liability protections in Section 230 of the Communications Decency Act which congress set up to foster a free and open internet. You think you're above the law because in a sense, congress gave you that power but congress gave you that liability shield to one end--that was the protection of innocent children. Catherine [sic] McMorris Rodgers knocked it out of the park today hammering the point where children are vulnerable.

Let's look at a John Doe vs. Twitter case that's ongoing right now. According to the National Center of Sexual Exploitation a teenage boy, a victim of child sex trafficking had images of his abuse posted on Twitter. One of those videos went viral and he became the target of bullying to the point of being suicidal. He contacted you to alert you that his sex-abuse images were on your platform. You failed to take them down. His mother contacted you to alert you and again, you failed to take them down. They called the police and they followed up with you with a police report. Your support center told the family that after review the illegal video was not a violation of your terms of service in the meantime, the illegal video accrued over 167,000 views. It took

[*]DUNCAN: a threat from Homeland Security agent to get Twitter to take down the video. Even then you took no action against the accounts that were sharing it and continue to share sexually explicit videos of minors in clear violation of the law and in clear violation of your duties under Section 230 of the Communications Decency Act as they were passed. So in the eyes of Twitter it's better to be a pedophile pornographer, a woke racist, or a state sponsor of terror than it is to be a conservative, even a conservative president.

You've abused Section 230 liability shield we gave you to protect children and used it to silence conservatives instead. As we've heard today your abuses of your privilege are far too numerous to be explained away and far too serious to ignore. So it's time for your liability shield to be removed. Your immuni--munity shield and immunity shield of other woke companies who choose to score political points with their immunity shields rather than protect children. My colleagues have been asking you if you deserve to continue to receive immunity under Section 230. Let me answer the question for you. No, you don't.

Y'all think you do, but you don't because you continue to do a disservice to that law and its intent. The United States Constitution has the 1st Amendment and that should be your guide. Protecting the speech of users of your platform instead of treating them like hostages and forcing things through algorithms to lead them down a path. The American people really are tired of you abusing your rights, abandoning the--their values.

So one of the Christian leaders that you banned, Mr. Dorsey, had as her last post a scripture verse that you took down. And I wanna leave it with you here today. Psalm 34:14. Depart from evil and do good. Seek peace and pursue it. Rather than silence that wise advice I strongly suggest that you follow it.

Now I've heard a lot of stuff on this hearing today about 230 protections. I challenge my colleagues to really get serious about doing something about this liability shield so that we do have a fair and free internet and people aren't censored. With that, Mr. Chairman, I yield back.

DOYLE: Gentleman's time is expired. The Chair recognizes Ms. Kelly for five minutes.

KELLY: Thank you Mr. Chair. Thank you to the witnesses for testifying today. The business model for your platforms is quite simple: keep users engaged. The more time people spend on social media the more data harvested and targeted ads sold. To build that engagement, social media platforms amplify content that gets attention. That can be cat videos, or vacation pictures. But too often it means content that's incendiary, contains conspiracy theories, or violence.

Algorithm--algorithms in your platforms can actively funnel users from the mainstream to the fringe, subjecting users to more extreme content all to maintain user engagement. This is a fundamental flaw in your business model that mere warning labels on posts, temporary suspension of some accounts, and even content moderation cannot address. And your companies' insatiable desire to maintain user engagement will continue to give such content a safe haven if doing so improves your bottom line.

I'd like to ask my first question of all the witnesses. Do each of you acknowledge that your company has profited off harmful misinformation, conspiracy theories, and violent content on your platform? Just say yes or no. Starting with Mr. Dorsey, yes or no.

DORSEY: No. That's not our business.

KELLY: Mr. Zuckerberg.

ZUCKERBERG: No, Congresswoman, I don't think we profit from it. I think it hurts our service.

KELLY: Mr. Pichai.

PICHA: Congresswoman, certainly not our intent and we definitely do not want such content and we are capable of (INAUDIBLE)--

KELLY: --Well, since you all said no can you please provide to me in writing how you manage to avoid collecting revenue from ads either targeted by or served on such content? So I will be expecting that.

There's a difference between a conversation in a living room and one being pumped out to millions of followers from discouraging voting and COVID-19 misinformation, to encouraging hate crimes and violence. The harms are real and disproportionate. Do you acknowledge that such content is having especially harmful effects on minority and communities of color? Yes or no again. I don't have a lot of time so yes or no. Mr. Dorsey.

DORSEY: Yes.

KELLY: Mr. Pichai.

PICHAJ: Yes.

KELLY: Mr. Zuckerberg.

ZUCKERBERG: Yes, I think that's right.

KELLY: Thank you. If your financial incentive is (INAUDIBLE) in human psychology lead to the creation of a system that promotes emotionally charged content that is often harmful do you believe that you can address them or do you believe that you will always need to play more of a whack a mole on different topics? Mr. Zuckerberg.

ZUCKERBERG: Congresswoman, I--I do think that we can take systemic actions that help to reduce a large amount of this. It--but there will always be some content that gets through those systems that we will have to react to.

KELLY: Mr. Dorsey.

DORSEY: The--the--it's not our incentive but I agree with Mark. We, you know, our--our model is to constantly iterate. We're gonna miss some things and we'll go too far in some cases.

KELLY: Mr. Pichai.

PICHAJ: I--I agree largely with what Mark and Jack said and, you know, we--we terminated a lot of channels, we removed thousands of misleading election videos. There are many evolving threats and we are very vigilant.

KELLY: Okay. More transparency and research into the AI models you use is needed. I understand that they are constantly evolving and pri--proprietary, however thele--those obstacles must not be insurmountable. Would you agree to some type of tests to evaluate your procedures and technology for desperate--disparate impacts? And would you welcome minimal standards set by the government? I only have 44 seconds.

DORSEY: I'll go. You're not calling on us, but we--yes. We're--we're--we're interested in opening all this up and--and going a little--a step further and having a protocol. I don't think that should be government driven but it should be open and transparent that the government can look at it and understand how it works.

ZUCKERBERG: And I agree that there--that this is an area where research would be--would be helpful and--and I think some standards especially amongst the civil rights community would be helpful guidance for the companies.

PICHAJ: Congresswoman, we work with many third parties, I just mentioned the hot collaboration we had. Definitely would be open to conversations about minimum standards, it's an important area.

KELLY: Thank you. I yield back--

DOYLE: --The gentlelady's time is expired. Chair now recognizes Mr. Dunn for five minutes.

DUNN: Thank you very much, Mr. Chairman. Many of the questions today deal with personal harms but there are long term economic and security harms to our country I'd like us to keep in mind as well. I represent Florida's second Congressional district which is proud to host a large presence of the U.S. military including civilian support companies.

One of these is Applied Research Associates, which is doing great work with our military in the field of artificial intelligence and machine learning. I agree with our nation's top national security experts on the critical importance of the United States maintaining its competitive edge in AI. And I share the concern of former Google

CEO Eric Schmidt who warned just a few weeks ago of the grave consequences should we lose that edge to China.

Leader Rogers led a bipartisan bill enacted last year, the American Compete Act, to lay out clear AI strategy. We all recognize the China is not a good place to do business, evidenced by the fact that all of your respective main products and services are banned there. It's—it's clear that the influence of the Chinese Communist Party permeates the entire corporate structure in China.

Xi Jinping himself stated his goal of integrating the party's leadership into all aspects of corporate governance. Let's be clear with each other, it's impossible to do business in China without either directly or indirectly aiding the Chinese Communist Party. It's also important to state for the record that each of your business models involve collecting data from individuals who use your product and then using that data for some other purpose.

Mr. Pichai, I'm deeply concerned with Google's pursuit of and investment in artificial intelligence research in China widely reported over the last few years. First and foremost, can you assure Americans that their personal data, regardless of how you think you have deidentified it, data you collect when they use Google and which is central to your algorithms is not used in your artificial intelligence collaboration with the Chinese government?

PICHAU: Congressman, I want to correct any misperceptions here. We do not have a AI research center in China now. We had a limited presence working on open source projects. Primarily on open sourced projects and around K-12 education a handful of employees we don't have that anymore. Compared to our—our peers we don't offer our core services in China products like search, YouTube, Gmail, etcetera.

DUNN: I'm going to have to reclaim my time because it's limited. But I want your team to follow up with me because I'm honestly somewhat skeptical. I think you had three centers there in China and I want to know more about what they're doing. And also, what material they're using. I want to be clear, I'm not suggesting that simply doing business in a country means that you endorse all of their policies. As a former businessman myself I know the political all too often get in the way of what we are trying to do.

However, Google's own list of artificial intelligence principles states that it will not collaborate on technologies that gather or use information for surveillance violating internationally accepted norms or contravenes widely accepted principles of international law and human rights.

But we know that the Chinese Communist Party is using artificial intelligence technology to spread misinformation and suppress the pro-democracy movement in Hong Kong. As well as using that technology in its genocidal crimes against the Uighurs including murdering them for their organ harvesting. You know, once again can you be sure that none of the work you are doing in collaboration with China, Chinese government is not aiding them in this ability?

PICHAU: Congressman, happy to follow up and clarify the limited work on AI we undertake. It's primarily around open source projects and very happy to engage in and very specifically follow up on what we do.

DUNN: Well, I think that's great and I know I'm running out of time here but I ask that—that we continue this dialogue. And I think Google would be very well served by promoting greater transparency in all of its actions regarding artificial intel—intelligence in China. Your—your customers have a right to know about this.

In 2018, Diane Greene former CEO of Google Cloud noted, we believe the uses of our cloud and artificial intelligence will prove to be overwhelmingly positive for the world. But we also recognize we cannot control all downstream uses of our technology. Well, a good place to start would be to end this dangerous artificial intelligence research relationship with China. With that, Mr. Pichai. Thank you all the members of the witness panel and Mr. Chairman I yield back.

DOYLE: Gentleman yields back. Chair recognizes Mr. McEachin for five minutes.

MCEACHIN: Thank you, Mr. Chairman and to you and Chairman Pallone and Chairman—Chairman Schakowsky—thank you for convening today's hearing and for our witnesses for joining us. In July of last year I led more than 30 of my colleagues, including several on this committee in a letter to your companies asking what you are doing to halt the spread of climate change disinformation on our platforms.

As my colleagues and I clearly expressed in our—in our letter, climate change is a real and urgent threat and the spread of disinformation on your platforms is undermining that fact. Since the World Health Organization estimates that cite change cause 150,000 deaths annually the number will only increase in the coming years.

All this begs a simple question--why do our platforms not treat climate change disinformation with a sense of immediacy and alarm? Mr. Zuckerberg, Facebook recently implemented the Climate Change Information Center which directs users to a landing page which climate--with climate change facts from researchers and organizations. Are you able to share data on how widespread a problem climate change disinformation is on our platform and how much the Climate Change Information Center has reduced it?

ZUCKERBERG: Sure thanks--thanks, Congressman. Our approach to fighting misinformation of which climate misinformation is a big issue. So I agree with your--with your point here. We take to a multipronged approach. One is to try to show people authoritative information which is what the climate information center does and then we also try to reduce the spread of misinformation around the rest of the service through this broad third-party fact-checking program that we have in which one of the fact-checkers is you know, is--is specifically focused on science feedback and climate feedback type of issues.

Overall, I'd be happy to follow up and share more details on--on what we have seen across those. But this is certainly a--an area that I agree is extremely important and needs multiple tactics to address.

MCEACHIN: Well, thank you. And it's my understanding that this climate center was modeled after your COVID-19 information center. However, different standards still apply for the organic content and paid for advertising for climate change versus COVID-19. One is faced with (INAUDIBLE) got to apply the same standards of fact checking on climate change that it does on COVID-19 content.

ZUCKERBERG: Congressman your--your right that the climate information center was based off our work on the COVID information center and election information center. In terms of how we treat misinformation overall. We--we divide the misinformation into things that could cause eminent physical harm, of which COVID misinformation that might lead someone to get sick or hurt or vaccine misinformation falls into the category of eminent physical harm and we take down that content.

And then other misinformation or things that are false but may not lead to eminent physical harm we label and reduce their distribution but leave them up. So, that's the broad approach that we have in that--that--that sort of explains the some of the differences between some of the different issues and how we approach them.

MCEACHIN: Mr. Pichai, I hope I'm pronouncing that correctly, sir--YouTube has employed contextualization tools linking viewers to similar sources as Facebook's climate center. That being said, you restricted but not removed some repeat offenders from your platform such as Prager University a non-accredited university producing climate change denial content. Are you not concerned about restricting those videos in--by restricting those videos and not removing repeat offenders the people who are determined to find those videos to validate their views will indeed find them and share them with others?

PICHAU: Congressman, it's an incredibly important area in--in general in these areas we rely on raising authoritative information both by showing information panels as well as raising scientific content, academic content and journalistic content. So our algorithms ranked those types of content higher for an area like climate change similar to (INAUDIBLE) and COVID. And you know, obviously it's an area where--where there is a range of opinions people can express. We have clear policies and if it's violated we remove. If it is not violated but if it is not deemed to be of high quality we don't recommend the content and that's how we approach it and--and we committed to this area. It's a company you know, we lead in sustainability. We have committed to operating 24/7 on a carbon free basis by 2030 and it's an area where we are investing significantly.

MCEACHIN: Well, thank you. I've run out of time. Mr. Dorsey, I apologize to you. Perhaps we'll have an opportunity to have a conversation. Mr. Chairman, I give you my two seconds.

DOYLE: I thank the gentleman. Gentleman yields back. Chair now recognizes Mr. Curtis for five minutes.

CURTIS: Thank you, Mr. Chairman and thank you to our witnesses. My first comment is to point out that in her 2019 presidential campaign, Senator Elizabeth--Elizabeth Warren, Democrat, called for the breaking up of your companies.

Several weeks ago at a speech at CPAC, Senator Josh Hawley, republican also said that big tech companies should be broken up. I don't think I need to point out the irony of Josh Hawley validating Elizabeth Warren at CPAC.

There seems to be a train wreck coming. Unfortunately, the very few tools that we have in our tool bag are regulation and breaking up. Mr. Zuckerberg, I read through your terms of service including the dense community standards document. In your terms of service you state that you cannot control and do not take responsibility for content posted on your platform. The community standards, which is frequently cited as why content is or is not censored says you sometimes make content moderation decisions based off what's considered best for the public interest or public discourse.

I know your testimony you said that companies need to earn their liability protections. That's great. But that doesn't address the concerns people understandably share about your past or current views on what is or is not acceptable. How do you claim you cannot take responsibility and therefore should maintain your liability protections for content posted on your site—but the same time state that your platform or monitor content based off what's in the public's best interest? That appears to be two sided.

ZUCKERBERG: Congressman, thanks. People use our services to share and—and send messages billions of times a day and it would be impossible for us to scan or—or understand that—that was going on and—and I don't think that our society would want us to take the steps that would be necessarily to—necessary to monitor every single thing. I think that we would think that that would infringe on our freedoms.

I think it's impossible to ask companies to take responsibility for every single piece of content that someone posts. And that I think is the wisdom of 230. At the same time, I do think that we should expect large platforms to have effective systems for being able to handle broadly speaking con—categories of content that are clearly illegal.

So we've talked today about child exploitation, and opioids, and sex trafficking, and things like that. And I think it's reasonable that—to expect that companies have systems that are broadly effective even if they're not gonna be exactly perfect and there are still gonna be some pieces of content that inevitably get through. Just like no police department in a city is going to be able to eliminate all crime.

CURTIS: I've gotta jump in only because we're out of time. I would love to spend more time on that with you. Let me also ask you, Utah's known for Silicon Slopes, our start-up community. You've called for government regulation but some view this with skepticism because larger companies tend to deal with regulation much better than small companies. If you think back to your college days, the early startup phase of Facebook, what challenges do you see for startups to compete and what cautions should Congress consider as we look at regulation that potentially could be a barrier for companies that just might be your future competition?

ZUCKERBERG: Thanks. I think that this is a really important point whenever we're talking about regulation. And I wanna be clear that the—that the recommendations that I'm making for Section 230 I would only have applied to larger platforms. I think it's really critical that a small platform, the, you know, the next student in a dorm room or in a garage needs to have a relatively low, as low as possible regulatory burden in order to be able to—to innovate and then get to the scale where they can afford to put those kind of systems in place.

So I think that that's a really important point to make. But I think that that goes for the content discussions that we're having around 230. But probably also applies to—the privacy law that I hope that Congress will pass in—in the—this year or next year to create a federal U.S. privacy standard. And I also think that—that—that we should be exploring proactively requiring things like data portability that—that would make it easier for people to take data from one service to another.

CURTIS: Thank you. I've got just a few seconds left and Mr. Pichai, this is a little bit off topic so I'm just simply gonna ask this question and submit it for the record and not ask for a response. Almost a decade ago your company started Google Fiber. You introduced Goog—gig speed and free internet to all the residents of my home city, Provo, Utah. Sadly, it seems like your efforts to do this across the country were slowed down or even stopped by excessive government regulations.

I'd love you to share off the record and—and I'll submit it for the record why government is making it so hard to expand internet across the country. Thank you, Mr. Chairman and I yield my time.

DOYLE: Gentleman yields back. The Chair recognizes Mr. Soto for five minutes.

SOTO: Thank you, Mr. Chairman. When television, radio, traditional newspapers, political blogs, and even private citizens spread lies they can be sued and held liable for damages or FCC fines. But pursuant to 230 you all can't be sued. You have immunity. But it ain't 1996 anymore, is it. Meanwhile sa—lies are spreading like wildfire through platforms. Americans are getting hurt or killed and the reason is your algorithms.

I want you to all know I--I was held captive in the Gallery during the Capitol insurrection. I was surrounded by domestic terrorists that killed the Capitol Police officer, ransacked the Capitol, and almost disrupted a Presidential election. And many of these domestic terrorists plotted on your platforms. I think we all understand by now this violence is real. And so this is why we're here today, in the committee or jurisdiction with power to protect our fellow Americans.

Mr. Zuckerberg had mentioned effective moderation systems, so now we know you have systems that can prevent many of these harms. Thank you for your statement supporting accountability today, and even for championing support accountability in ads. So the question is what specific changes to Section 230 do you support to ensure more accountability? Mr. Zuckerberg just mentioned categories of content that are clearly illegal. U.S. privacy standards and data portability is three standards we should be looking at.

Mr. Pichai, should we be creating these standards and then holding platforms accountable if they violate them under 230?

PICHA: Congressman, first of all there are many ways and there are many laws today which do hold us liable. You know, FTC has oversight, you know, we have consent decree with the FCC, COPA, HIPPA, et cetera. And for example, alias where there are privacy laws and we have called for federal privacy legislation. But in Europe a GDPR. In California, we have privacy state legislation. We are both accountable as well as we are subject to private plaintiff action against these statutes.

So--

SOTO: --So Mr. Pichai, you agree with these categories that were just allow--outlined by Mr. ge--Zuckerberg. Is that correct?

PICHA: I definitely think what Mark is talking about along the lines of transparency and accountability are good proposals to think through. There are various legislative proposals along those--

SOTO: --Thank you for your time. Mr. Dorsey, do you think we should be establishing categories of content that are clearly illegal? U.S. privacy standards and data portability as well as penalties for violation of those standards.

DORSEY: I--I believe as--as we look upon 230 and evolutions of it and putting upon it, I think we need more transparency around content moderation practices, not just the policies. I think we need more robust appeals processes and I--I think the real issue is algorithms and giving people more choice around algorithms, more transparency around algorithms.

So if there's anyone I would pick it would be--it would be that one. It's a tough one but it--it's the most impactful.

SOTO: Thank you, Mr. Dorsey. Mr. Zuckerberg, political misinformation spread rampantly unfortunately in Spanish in Florida's Hispanic community on Facebook in the 2020 Presidential election. Even with the political ad ban, how do you think this happened? Mr. Zuckerberg.

ZUCKERBERG: Congressman, it's, you know, I--I do still think that there is--that there's too much misinformation across all--all of these media that we've talked about today. Ha--how did it happen, I mean, it's, you know, I--I think we--we've talked a lot today about algorithms. But I actually think a lot of this stuff happens in wha--what we refer to as deterministic products like messaging. Right?

Someone sends a--a--a me--a text message to someone else. That's--it's--there's no algorithm there determining whether that gets delivered. People can just send that to someone else. A lot of this stuff I think unfortunately was amplified on tv and in traditional news as well. There was certainly some of this content on Facebook and it's--it's our responsibility to make sure that we're do--building effective systems that can reduce the spread of that.

I--I think a lot of those systems performed well during this election cycle, but there--it's an iterative process and there are always going to be new things that we--that we will need to do to keep up with the different threats that we face.

SOTO: Mr. Zuckerberg, will you commit to boosting Spanish-language moderators and systems on Facebook especially during election season to help prevent this from happening again in Spanish language?

ZUCKERBERG: Congressman, this is already something that we focus on. We--we already beefed up and--and added, you know, more capacity to Spanish language fact checking and Spanish language authoritative information resources. And that's certainly something that we hope to build on in the future. So I--the--the answer to your question is yes.

DOYLE: Gentleman's time is expired. The Chair now recognizes Ms. Lesko for five minutes.

LESKO: Thank you, Mr. Chair. And thank you to the witnesses. I represent constituents in the great state of Arizona. And most of my constituents just want to be treated fairly, equitably, impartially, and they wanna make sure that their private information stays private. Mr. Pichai, does Wikipedia influence Google's search results?

PICHAJ: We--we do index and Wikipedia is in our index and for certain queries if it can be--if an answer from Wikipedia rises to the top of our ranking yes, we do--we do rely on it.

LESKO: Thank you. Mr. Dorsey, did you personally decide to ban President Trump from your platform?

DORSEY: We have a--we have a process that we go through to--to get there and--and that came after a warning.

LESKO: And did you make the final decision?

DORSEY: Ultimately I have final responsibility.

LESKO: Thank you. And Mr. Pichai, in July 2018 the Wall Street Journal reported that Google let hundreds of outside developers scan the inboxes of millions of Gmail users. Mr. Chipai--Ch--Pichai, do Google employees review and analyze Gmail users' content?

PICHAJ: Congresswoman, I mean, we take privacy very seriously. We--we don't use the data from Gmail for advertising. In our employees generally do not access it, only a narrow cases, either to troubleshoot with the right consent and permissions. You know, there are permissions with enough checks and balances--

LESKO: --So I think what you're saying is occasionally your employees do review and analyze. I have another question regarding that. Do you--does Google share Gmail users' emails or analysis of your emails with third parties?

PICHAJ: We do not sell any data. I think what you're referring to is users who give API access to third-party developers. For example, there are applications which could give travel related information. So, this is a user choice, and it's an API on top of the platforms. We have done numerous steps to make sure users have to go through multiple steps before they would give consent to a third party.

LESKO: And so, I've looked through your Google privacy statements and user content, and I still have concerns about that. I'm very concerned. I have Gmail accounts, just like millions of people. And I don't know if you're looking at them. I don't know who's looking at them. I don't know whose it sharing them. I don't know what you're doing with them.

PICHAJ: If I--

LESKO: --It makes me concerned. Mr.--I only have a--

PICHAJ: --If I could clarify one thing I said there--

LESKO: --Yeah--

PICHAJ: --Only if a user asks us to troubleshoot an account without user permission. But we do not look into users' email content and we do not share the contents with anyone else without the users asking us to do so.

LESKO: However, the Wall Street Journal had this article saying that hundreds of developers were reviewing the email contents. So, I have to move on to another question because I only have a short time.

Mr. Dorsey, Twitter denied the Center for Immigration Studies the ability to promote four tweets that contain the phrases illegal alien and criminal alien, even though those are the correct legal terms. Mr. Dorsey, if there is a warning posted related to a border threat, how will Twitter algorithms react to the use of the word illegal versus undocumented?

DORSEY: Well, it's not--it's not about our algorithms. It's interpretation against our policy and if there's violations. But we can follow up with you on how we'd handle situations like that.

LESKO: Well, it--you know, this is a legal term is illegal alien. That is in law and legal terms of. So, I don't understand why you would not allow that. That is the legal factual term.

And with that, I'm going to ask question. Mr. Zuckerberg, this has been brought up before. Do you believe that your platform harms children?

ZUCKERBERG: Congresswoman, I--I--I don't believe so. This is something that we study and we care a lot about. Designing products that improve people's well-being is very important to us, And what our products do is help people stay connected to people they care about, which I think is--is one of the most fundamental and important human things that we do, whether that's for teens or for--for people who are older than that. And--and again, our policies on--on the main apps that we offer generally prohibit people under the age of 13 from using the services.

DOYLE: The gentlelady's time is expired. The chair now recognizes Mr. O'Halleran for five minutes.

O'HALLERAN: Thank you, Mr. Chairman. I--I am enlightened--thank you to the panel today. I'm enlightened by what I've heard today. Three of the most knowledgeable businesspeople in the world with beautiful profit centers and business models, a sense of the future direction that your company's want to go in, standards that are in many cases reliable but others not very much so, and a very big concern by the Congress of the United States on the direction you want to go in versus what's good for our nation in total.

Mr. Zuckerman [sic], last October Facebook announced that it removed a network of 202 accounts, 54 pages, and 76 Instagram accounts for violating your 48 inauthen--inauthen--inappropriate behavior policy. Really, they're--the Forge Net--really Forge Network was based in Arizona and ran it's disinformation operation from 2018 to 2020 by creating fake accounts and--and commenting on other people's content about the 2018 midterm election, the 2020 presidential election, COVID-19, and criticism for--and praise of creation--certain political parties and presidential candidates. Sadly, Facebook only acted after a Washington Post investigation reported its findings.

While your testimony states since 2017 Facebook has removed over 100 networks of accounts for engaging in coordinated inauthentic behavior, where did Facebook fail by not finding this network over the course of a number of years?

ZUCKERBERG: Well, Congressman--

O'HALLERAN: --Was that--

ZUCKERBERG: --We have a team of--you know, I think it's more than 300 people who work on counterterrorism at this point and--and--and basically trying to work with law enforcement and--and across the--the--the industry to--to basically find these networks of--of fake accounts and inauthentic accounts that are trying to spread behavior. And I think we've gotten a lot more effective at this.

It's--you know, I--I--I can't say that we catch every single one, but--but certainly I think we've done a lot more effective, including there just this week that we announced that we took down a--a network of--of Chinese hackers that were targeting Uyghur activists outside of China.

So, we've got more sophisticated at this. Sometimes when we start finding a lead we--we need to wait's to kind of see the full extent of the network so we can take down the whole network. So, that's a--a trade-off that, you know, sometimes we--we are able to discuss with law enforcement and other times not in terms of how we do enforcement. But--but overall, I think this effort has gotten a lot more sophisticated over the last four years.

O'HALLERAN: So, you're happy with the amount of personnel that you have working on these issues?

ZUCKERBERG: Congressman, I think we have one of the leading teams in this area. You know, we went from more than four years ago--

O'HALLERAN: --Are you happy with--the question was are you happy with the amount of people you have working in that capacity that you have to take care of these issues?

ZUCKERBERG: Congressman, I--I think the--the team is--is well staffed and--and well-funded. We spend billions of dollars a year on--on these kind of content and integrity and security issues across the company, so I think that that is appropriate to meet the challenge. And there are always things that we're going to want to do to improve the tactics of--of how we find this. And a lot of that over the last several years has been increasing the work that we do with law enforcement and the--and the intelligence community in the--

O'HALLERAN: --I'm going to move on to another question, Mr. Zuckerman [sic]. Thank you very much. I--I do want to say that, again, you're a bright, intelligent CEO. You know in advance what you want. Your algorithms are created by your company and--and the other companies. You have control over the algorithms.

And so, the idea that--that you're--kind of have to work maybe in this direction, Mr. Zuckerman [sic], Facebook's most recent community standards enforcement report states that 2.5 million pieces of content related to suicide and self-injury were removed in the fourth quarter of 2020 due to increased reviewer capacity. You can do this if you want to do all this stuff.

Very briefly explain what policies Facebook put in place to increase the reviewer capacity not just on that issue but across the respect how much overtime has this occurred that you continue to increase reviewer capacity?

ZUCKERBERG: Sure, Congressman. The--the biggest thing that we've done is augmented a lot of this by building AI tools to identify some of this. So, you know, now, you know, for example more than 95 percent of the hate speech that we take down is--is done by an AI and not by a person. And I think it's 98 percent or 99 percent of the terrorist content that we take down is--is identified by an AI and not a person. And you mentioned the suicide content as well, which, you know, I think a high 90s percent is identified by AI rather than--

O'HALLERAN: --Mr. Zuckerman, I'm over my time. I want to thank the chair and I also want to stay very briefly that you have a lot of work to do and--you and your--your other cohorts on this panel. Thank you.

DOYLE: The gentlemen's time has expired. Chair recognizes Mr. Pence for five minutes.

PENCE: Thank you, Chairs Doyle and Schakowsky and Ranking Members Latta and Bilirakis for holding this joint committee hearing. And thank you to the witnesses for appearing before us today. The extent to which your platforms engulf our lives is reminiscent to the all-encompassing entities we've seen over the past century. In the early 1900s, Standard Oil had a monopoly over 90 percent of our country's refining business. By the 1970s, if you used the telephone it was going to be Ma Bell system. In each instance you could choose not to use either product but participation in society demanded that you use both. In a similar sense, it is difficult if not impossible to participate in society today without coming across your platforms and using them.

We could choose not to use them but like oil and telecommunications it's considered essential and so many other people do use it. Even the government has become an equal contributor. I Each member of congress and very senator is all but required to use your platforms to communicate with their constituents while we're in Washington D.C. I know you understand that your platforms have a responsibility to act in good faith for Hoosiers and all Americans.

Unfortunately, regularly my Facebook and Twitter accounts, like many of my peers and other people I know are littered with hateful, nasty arguments between constituents that stand in complete opposition to the ideas of civil discourse that your platforms claim to uphold and that you referenced today.

I'm sure you are aware that official government accounts have restrictions that significantly limit our ability to maintain a platform that is a productive resource of information to the public. They have essentially become a micro town hall without a moderator on social media. I agree with all your testimonies that a trust deficit has been growing over the past several years and as some of you have suggested we need to do something about it now.

The way in which you manage your platforms in an inconsistent manner, however, has deepened this mistrust and evolved the public conversation. My constituents in Southeast Indiana have told me they are increasingly mistrustful of your platforms given how you selectively enforce your policies. There is just a few examples of how this has occurred. Members of the Chinese Communist Party have verified Twitter accounts to regularly pedal false and misleading claims surrounding the human right--human right violations we know are occurring in Northern China.

Twitter gives the Supreme Leader of Iran a megaphone to proclaim derogatory statements endorsing violence against U.S. and western culture. Twitter accounts associated with the Supreme Leader have called Israel a cancerous tumor and called for the eradication of the Zionist regime.

This happens as he also bans a service for his own people to restrict their free expression. Mr. Dorsey, you need to do more to address content that violates your policies. I have two questions for you--why is the Chinese Communist Party allowed to continue the use of your platform after pushing propaganda to cover up human rights abuses against Muslims in Northern China? And two, why does the Supreme Leader of Iran still have a platform to make threats against Israel and America?

DORSEY: So--so first and foremost we do--we do label those Chinese accounts so that people have context as to where they are coming from. That's on every single tweet. So people understand the--the source. We think that's important. We are reviewing our world leaders policy. We're actually taking public comment review right now so we're enabling anyone to give us feedback on (INAUDIBLE).

PENCE: If I may interrupt you quickly, Mr. Dorsey--on--on that very point, you know, Iran has been supporting--supporting Hezbollah and it's not just saber rattle--rattling as--as you've made the statement or your company has made the statement. They have done serious damage to whole countries and people and as I served in the military they--they killed hundreds of Marines many years ago. So I don't know what you have to study about this.

Mr. Chairman, I yield back.

DOYLE: Gentleman yields back. Chair recognizes Ms. Rice for five minutes.

RICE: Thank you, Mr. Chairman. Mr. Dorsey what is winning yes or no on your Twitter account poll?

DOYLE: Yes.

RICE: Hm. Your multitasking skills are quite impressive. In December of 2020 the House committee on veterans affairs released a report entitled High jacking our Hearings exploiting veterans through misinformation on social media. I ask unanimous content--consent, Mr. Chairman, that this report be submitted for the record.

DOYLE: So ordered.

RICE: Thank you. I bring up the report today because it's very disturbed--deeply disturbing the involvement of our veterans and and military service members in the violence that took place on January 6th. It's estimated that one in five people charged in connection with the attack have served or--or are currently serving in the U.S. military. It should come as no surprise to those testifying today that for years nefarious actors have learned how to harness the algorithms on all of your platforms to introduce content to veterans and military service members that they did not actively seek out for themselves. Veterans and military service members are particularly targeted by malicious actors online in order to misappropriate their voices, authority and credibility for the dissemination of political propaganda.

We have to do better for those who have served our country. Mr. Zuckerberg, do you believe that veterans hold a special status in our communities and have military training making them prime targets for domestic terrorist and our adversaries seeking to foment insurrection?

ZUCKERBERG: Congresswoman I--I certainly believe that veterans hold a special place in our--in our society. I haven't seen much research--

RICE: Did you get on the National--did you see on the National Mall and at the Capitol there were rioters who arrived in combat gear who were armed with tactical equipment. Did you see those images yes or no?

ZUCKERBERG: Yes.

RICE: OK. Have you personally talked to the Iraq and Afghanistan veterans of America IAVA about disinformation campaigns targeting veterans?

ZUCKERBERG: No, Congresswoman, I have not personally although our--our team certainly is--is in contact with a number of these groups as we set up our policies.

RICE: Have you talked to the Vietnam Veterans of America about disinformation campaigns targeting veterans/

ZUCKERBERG: Congresswoman, I can get back to you on whether our team has--has consulted with them specifically, but broadly what our teams--

RICE: Do you believe that veterans and military service members are just like other Americans in that they are susceptible to the impulses of human psychology that Facebook exploits to drive engagement--do you believe that they are susceptible in that way? Yes or not?

ZUCKERBERG: Congresswoman there is a lot in our characterization there that I disagree with.

RICE: Do you think they are susceptible to that kind of information coming at them yes or no?

ZUCKERBERG: Congresswoman I believe that--that--that--

RICE: OK. So given your answers I'm not convinced that you have the appropriate resources devoted to the problem of mitigating the real world effects of content that I designed to mislead and radicalize your users--especially those who are veterans and military service members. Would you support legislation that require you to create an office of veterans affairs that reports to the CEO and works with outside veterans service organizations to ensure our enemies don't gain ground trying to radicalize our brave men and women who serve in our military? Would you support that--that legislation?

ZUCKERBERG: Congresswoman, I think the details matter a lot. So I would--I would be happy to follow up with you or have our team follow up with your team to discuss this but in general I do think that--

RICE: (INAUDIBLE) I will take you up on that Mr. Zuckerberg. It's just a broad stroke. Do you believe that you could find your way to support legislation that would have as its goal the protection of our military active duty and veterans?

ZUCKERBERG: I think in principle I think something like that could certainly make sense.

RICE: So I wrote to you, Mr. Zuckerberg, last month requesting information about Facebooks' effort to curb disinformation campaigns as specifically targeting American service members--and veterans I'm just curious if you know how many public groups with the word veteran or public pages with the word veteran--did you remove from your platform after January 6th in association with misinformation about the 2020 election or the attack on the Capitol?

ZUCKERBERG: Congresswoman, I don't know the answer off the top of my head but I would be happy to get back to you with that.

RICE: Thank you. Thank you. I we believe that you should be tracking that information. Your platform was, in fact, a crime scene after January 6th and we need that information and data to understand how the attack happened. I want to thank all three of you for coming here today and spending so much time with us. I yield back. Mr. Chairman. Thank you.

DOYLE: Gentlelady yields back. Chair recognizes Mr. Armstrong for five minutes. Is Mr. Armstrong here?

You need to--you need to unmute, Kelly.

ARMSTRONG: All right. Sorry about that. Can you hear me?

DOYLE: Yes, we can hear you.

ARMSTRONG: All right. Thank you. No other industry received such bipartisan scrutiny. Disinformation content moderation, de-platforming, antitrust, privacy, and the list continues to grow. We discussed these things too often in isolation, but they're all related. And it starts with the fact that your users aren't your customers. They are the product.

More specifically, the data that you collect from your users as the product. You're incentivized to collect and monetize user data for behavior advertising. This results in the collection of even more user data. And data is--data is unique as a business asset. It doesn't deplete. Data is perpetual and reinforcing. Data begets more data. Massive data collection expands your market share, which harms competition. That's why censorship is so concerning to all of us.

Your platforms have a stranglehold on the--on the flow of modern communication, and I think we absolutely have to resist the urge of content moderation and censorship. In 1927, Justice Breyer--1927 Justice Brandeis wrote, "The remedy do apply is more speech, not enforced silence." I think that statement still holds true today.

Yet, your platforms don't simply silence certain speech. Your algorithms are designed to reinforce existing predisposition--predispositions, because you profit by keeping users locked into what they already enjoy. This leads to information silos, misinformation, extremism on both sides, and even more data collection, which--which repeats the cycle.

Mr. Pichai, you testified before the House Judiciary Committee last year, and at that hearing, I raised several examples of Google's consolidation of the Ad--Ad tech stack. Your answers largely reiterated the privacy justification, which I understand and support. However, my question was whether Google's consolidation of both a buy and sell sides of digital advertising would further harm competition.

Since then, I have reviewed Google's privacy sandbox and the FLoCs proposal, which is an alternative group identifier to replace third party cookies. Again, I understand and I appreciate the privacy justification. But--and this is my question, how will these actions not further entrench Google's digital advertising market share and high-harm competition?

PICHAU: Congressman, as you rightfully point out, privacy is really important, and we are trying to get that correct. Users are giving clear feedback in terms of the direction they would like to take. Advertising allows us to provide services to many people who wouldn't otherwise be able to use services and--and we are trying to provide relevant ads, protecting their privacy. And that's what FLoC is working on. We will--

ARMSTRONG: --I--I'm going to move on. Because I understand the privacy--I understand the privacy. And I understand the rationale of eliminating individual level tracking in favor of cohorts and the potential privacy benefits of user data at the--at in Chrome at the device level. But this--but this is still eliminating competitor's access to user data at a time when you are ready control 60 percent of the browser market.

I have real concerns, that FLoCs will incentivize more first party data collection, which will not actually benefit user privacy, instead of spreading it amongst a lot of different companies. It will just all be--it'll all be with you. And so I guess my point is Congress needs to conduct careful oversight as the privacy sandbox, and FLoCs are introduced. And we need to ensure that the user privacy increases and that competition is not stifled further.

But I do have one question. And it's important. I'm going to ask all three of you. When we're conducting competition analysis in the tech industry, should non price factors like privacy be considered? And I'll start with you Mr. Pichai?

PICHAU: I think so. I think privacy is very important. And, you know, we've called for comprehensive federal privacy legislation. And to clarify, Google, or--Google doesn't get any access to FLoC data, which (INAUDIBLE) is protected. You know, and then you will publish more papers on it.

ARMSTRONG: I--I--and I understand completely, but you're forcing, I mean, you're forcing advertisers into the ad stack. I mean, that's the--I mean, it's--I don't discount it--it increases privacy. That's--I think this is a real problem, because I think they're in contact--conflict with each other. But Mr. Dorsey, do you think when we're conducting competition analysis in the tech industry, non-price factors should be considered?

DORSEY: I'm not sure exactly what you mean, but open to a further discussion on it.

ARMSTRONG: All right. How about you, Mr. Zuckerberg?

ZUCKERBERG: Yes, Congressman. And my understanding is that the law already includes the quality of products in addition to price.

ARMSTRONG: And I will just say, I appreciate you talking about the difference between big platforms and small platforms. Because I think when--in our history of trying to regulate big companies, Congress has always done a really good job at harming the smaller companies worse. And with my last six seconds, because this isn't the appropriate hearing, but I'm going to ask, please all do a better job of making sure artists get paid for their work on your platforms. And with that, I yield back.

DOYLE: The gentleman yields back. The Chair recognizes Mr. Veasy for five minutes.

VEASY: Thank you, Mr. Chairman. It's often been said that lies travel faster than truth. And we've seen that play out with devastating consequences on social media platforms today. This concerns me greatly not just as a father or a lawmaker, but as someone ready to see the past divisions that have dominated our country for the past several years, and really, decades, really.

But it's hard to see how this can change. I want the CEOs of the largest social media platforms repeatedly say they will fix their ways only to keep spreading harmful lies and misinformation. I want to give you an example, last August here in the Dallas Fort Worth area, the North Texas Poison Control Center felt the need to warn people against ingesting bleach or other disinfecting products as a cure to prevent COVID-19. Despite efforts of your companies to take down such harmful mis or misinformation calls to the north Texas Poison Control Center about disinfectant, ingestion rates were much higher than usual and statewide calls about bleach products were up over 70 percent compared to the year before.

The North Texas Poison Center pointed out largely--pointed this out largely to misinformation online as the cause for these increases. And as we know in the lead up to last elections, black communities were specifically targeted for disinformation campaigns designed to suppress the vote, especially in battleground states. And right now there are sites up that are discouraging black people from getting the COVID-19 vaccination.

I know a lady that was put in Facebook Jail for 30 days, because all she did was repost one of the faulty posts when--saying black folks--black folks aren't falling for this BS. And she was put in Facebook Jail for 30 days. Now--and now, even if these posts were eventually taken down or otherwise labeled as false, again, lies travel a lot faster than then truths. Your companies have been largely flat footed when it comes to getting out ahead of these issues. And it's time for something to change.

That's why I'm exploring legislation that would establish an independent organization of researchers and computer scientists who could help identify and warn about misinformation trends before they become viral. This early warning system would help social media sites, the public, and law enforcement so that when dangerous conspiracies or disinformation is spreading, they can be on alert and hopefully stop--and hopefully slow its effect. Mr. Zuckerberg, would you support legislation that would alert all Facebook or Instagram users of harmful disinformation and conspiracy theories spreading across your platforms?

ZUCKERBERG: Congressman, I think we need to look into that in--in--in more detail to understand the nuances. But I, in general, I agree that it's our responsibility to build systems that can help slow the spread of this kind of misinformation. And that's why we've taken all the steps that I've outlined today from building an unprecedented independent fact checking program to taking down content that could cause imminent physical harm to the work in the COVID Information Center and the Voting Information Center in the Climate Information Center to promote authoritative information across our services. So I--I certainly think that there's a lot to do here.

VEASY: Mr. Dorsey, would you support legislation for an early warning system across Twitter?

DORSEY: I'd be open to reviewing the details. I just don't think it'll be effective. And it'll--it'll be very much whack-a-mole. And I think the more important thing is to, as I said in my opening remarks, like, get much more of an open standard and protocols that everyone can have access to and review.

VEASY: And Mr. Pichai for Google and YouTube as--and--and I have a 14-year-old at home that watches YouTube, what about you for--for those platforms?

PICHAU: We already today, in many of these areas, we show proactively information panels. So for example, on COVID we showed a lot of information from CDC and other experts, and we had views of over 400 billion and so, you know, conceptually showing proactive information, including information panels, I think--I think makes sense to me.

VEASEY: Well, thank you. I appreciate the time, Mr. Chairman. I'm just, I'm worried. I think that--that--that we need to act quickly and that we're running out of time. And that we need these companies to take affirmative action on addressing some of these issues. I yield back my time. Thank you.

DOYLE: Thank you, gentlemen. Gentleman yields back. The chair now yield five minutes to Ms. Craig.

CRAIG: Thank you so much, Mr. Chair. Mr. Zuckerberg, thank you so much for joining us today. As co-chair of the LGBT-LGBTQ Equality Caucus in the U.S. Congress, I'd like to ask you a few questions about an incident that occurred several weeks ago, now. And I would appreciate a simple yes or no answer.

Most of these have absolutely no room for nuance. These aren't trick questions. I just like to clarify a few facts. So, on February the 25th, Facebook took down a video hosted by my colleague, Representative Marie Newman, in which she places the transgender flag outside her office. Is that correct, to your knowledge? Yes or no?

ZUCKERBERG: Congresswoman, I'm--I'm not aware of this.

CRIAG: You're not aware of this?

ZUCKERBERG: No.

CRAIG: Well--well, the--the--the answer is yes. Facebook took her video down. According to rest--Representative Newman, the reason Facebook gave for taking down the video, was that it violated Facebook's community standards on hate speech and inferiority. Does that seem right to you, that if someone put up a trans flag and took a video of it and posted it on your platform, that it should be put down?

ZUCKERBERG: Congresswoman, that doesn't seem--that doesn't seem right to me, but I would need to understand the specifics of the case in--in more details.

CRAIG: Yeah, thank you. The--the answer is no, it's absolutely not right. Meanwhile, across the hall, Representative Marjorie Taylor Green from Georgia, posted a video to Facebook. Her video showed her putting up a transphobic sign so that representative Newman, the mother of a trans child could quote, "look at it every time she opens her door", close quote. Facebook allowed representative Green's video to remain online. Is that right? Yes or no?

ZUCKERBERG: Congresswoman, I'm not aware of the specifics. But as I've said a number of times today, we do you make mistakes, unfortunately, in--in our content moderation, and--and we hope to fix them as quickly as possible, when we do.

CRAIG: Reclaiming my time. Reclaiming my time. The answer was yes. Representative Greens video was allowed to remain online. Representative Newman reached out to Facebook and a few hours later, her video was restored with a perfunctory apology, but representative Greene's video was never taken down.

I'm not even going to ask you if I'm getting that right, as I was, because you obviously don't know. Are you aware that Facebook has repeatedly flagged the transgender flag as hate speech and that trans positive content ends up being taken down, while transphobic content like representative Greene's video is not taken down, it is often shared widely? Yes or no?

ZUCKERBERG: Congresswoman, I'm not aware of that, specifically. But this is an--an instance of a broader challenge in identifying hate speech, which is that there's often a very nuanced difference between someone saying something that's racist versus saying something to denounce something that someone else said that was racist. And we need to build systems that handle this content in more than 150 languages around the world. And--and we need to do it quickly. And unfortunately, there--there are some mistakes in trying to--trying to do this quickly and--and effectively.

CRIAG: Mr. Zuckerberg, I'm going to give you your nuance this one time. As it exists today, do you think your company is going to get these content moderation decisions right, on the first try, eventually?

ZUCKERBERG: Congresswoman, if what you're asking is, are we ever going to be perfect? The answer is no. I think that there will always be some mistakes, but I think we will get increasingly accurate over time. So, for example, a few years back, we--

CRAIG: Mr. Zuckerberg, I--I only have a couple of minutes, or one minute left, so I'm going to continue here. As it's been mentioned repeatedly throughout today, we just don't have faith that your companies have the proper incentive to proactively contemplate and address basic human rights. With that in mind, would you support legislation requiring social media companies to have an Office of Civil Rights reporting to the CEO, and that would mean you would have to reconsider your corporate structure, including the civil rights and human rights of trans--the trans community?

ZUCKERBERG: Congresswoman, we took the unprecedented step of hiring a VP of Civil Rights. And I think we're one of the only companies that has actually done something similar to what you're--what you're saying.

CRAIG: Well, I--I hope that that you do better then. Because this example I'm giving you was completely unacceptable. This panel has done something truly rare in Washington these days, it's united Democrats and Republicans. Your industry cannot be trusted to regulate itself. And with that, I yield back.

DOYLE: Gentlelady yields back. The Chair now recognizes Ms. Trahan for five minutes.

TRAHAN: Thank you, Mr. Chairman. I'd like to turn the focus back to our children. You know, my husband and I have five, our--our oldest is 27, our youngest is six. And over the years, I've noticed how technology has been increasingly designed to capture their attention. The more time my first grader spends scrolling through an app, the less time she is playing outside, or enjoying face to face interactions with us.

Google and Facebook are no--not only doing a poor job of keeping our children under 13 off of YouTube and Instagram, as my colleagues have already mentioned today, but you were actively onboarding our children onto your ecosystems with apps like YouTube Kids, Facebook Messenger kids, and now, we're hearing Instagram for kids. These applications introduce our children to social media far too early and include manipulative design features intended to keep them hooked. Mr. Pichai, when a child finishes a video on YouTube or YouTube Kids, does the next video automatically play by default? And I think this one is a yes or no.

PICHAJ: Sorry, I was muted. Congresswoman, I have children too. I worry about the time they spend online, and I agree with you. It's an important issue.

TRAHAN: Yes. The auto play--the auto play function, by default, that's a yes?

PICHAJ: On the main app, it is there. And for each video there is easy on off toggle users have preferences--

TRAHAN: --but the default setting is yes. When a user who is predicted to be a teen is watching a YouTube video, are the number of likes displayed by default, yes or no, please.

PICHAJ: On all videos, I think we do have--across all videos we have.

TRAHAN: Great and Mr. Zuckerberg, will the recently reported Instagram app for kids have endless scroll enabled, yes or no?

ZUCKERBERG: Sorry. Congresswoman, we--we are not done finalizing what the app is going to be, if--we're actually still pretty early in designing this. But yeah, I--I just want to say that--

TRAHAN: --are you not--are you not sure or you're not sharing features? Because--or look, another feature of concern is the filter that adds an unnatural but perfect glow for my 10-year-old to apply to her face. Is that feature going to be part of Instagram for kids?

ZUCKERBERG: Congresswoman, I--I don't know, I haven't discussed this with the team yet.

TRAHAN: Well, I--look, I--please expect my office and many others to follow up, given what we know about Instagram's impact on teen mental health. You know, we're all very concerned about our--our younger children. And, you know, just--I just want to speak mother to father for a moment, fathers, because leading experts all acknowledge that social media sites pose risks to young people.

Inappropriate content, over sharing of personal information, cyber bullying, deceptive advertising, the list goes on, and those risks are exacerbated with more time children spend in these apps. You know, Mr. Pichai, you mentioned that you have children, and that I've also read you limit your screen time. What do you say when one of your children doesn't want to put their phone down?

PICHAJ: Congresswoman, the struggle is the same, particularly through COVID. It's been--it's been hard to moderate it. And I do take advantage of the parental controls and the digital well-being tools, we can limit the time on their apps. And so, we have provisions in place.

TRAHAN: Understood. I don't mean--I don't mean to cut you off, Mr. Pichai, you know, but the last thing overworked parents need right now, especially right now, are more complex to do's, which is what parental controls are. I mean, they need child centric design by default. Mr. Zuckerberg, I understand your children are younger, but when they start using social media, what will you say when they're craving their tablet over spending time face to face with you or with friends.

ZUCKERBERG: Well, Congresswoman, we've haven't gotten to that point yet. But the--we're designing all of these tools--we designed Messenger Kids that the parents are in control. I think we've proven that that can be a good and safe experience and I think that was one of the things that--that made us think that we should consider doing this for Instagram as well by having it so that we have a parent-controlled experience. And as you say, child-centric experience for people under the age of 13--

TRAHAN: --Sir, I'm gonna re--I'm going to re--

(LAUGHTER)

TRAHAN: --I am going to reclaim my time only because connecting with others is one thing. Adding filters, no breaks for--for kids to take and, you know, manipulating the design of these apps for our children is--is another. Look, this committee is ready to legislate to protect our children from your ambition. You know, what we're having a hard time reconciling is that while you're publicly calling for regulation, which by the way comes off as incredibly decent and noble, you're plotting your next frontier of growth which deviously targets our young children and while you all take great sti--great strides with infinite--infinitely more resources in protecting your own children.

This playbook is fa--familiar. As some of my colleagues have already pointed out, it's the same tactic we saw from alcohol companies and big tobacco. Start 'em young and bank on them never leaving. Or at least never being able to. But these are our children. And their health and well-being deserve to take priority over your profits.

DOYLE: Gentlelady's time is expired--

TRAHAN: --Thank you Chairman--thanks for that.

DOYLE: Chair now recognizes Ms. Fletcher for five minutes.

FLETCHER: Thank you, Chairman Doyle. And thanks to you and Chairwoman Schakowsky and Ranking Members Latta and Bilirakis for holding this hearing today. I agree with my colleagues, there's a broad consensus on a range of issues and I appreciate the discussion. As we've discussed extensively today, one of the big challenges of this rise of dangerous disinformation is that it denies us a basic set of shared facts to enable informed debate like what we are having here today.

And it's absolutely vital that we take charge and that we address this. You know, what we've seen is that countries whose interests are not aligned with ours, extremist organizations, and others have used online social media platforms to engage and to amplify extremist content and disinformation. From the COVID-19 pandemic to the January sixth insurrection, both of which we've talked about extensively today, you know, we've seen that the real world cost of this unchecked spread of disinformation is in lives.

And like my colleagues I worry that the structure of many social media companies including those we have before us today prioritize engagement, including engagement with provocative or extremist content over responsible corporate citizenship. So, you know, one of my greatest concerns regarding how extremist content and disinformation is allowed to spread on your platforms is the lack of data transparency when it comes to independent analysis. You know, everyone has claimed they have an internal system, that it's about the systems, that you need good systems to remove and delete disinformation and extremist content.

But we have no way to verify how effective those systems are. And that's a--a huge part of the challenge before us. I--I think we all would agree that we need data and information to make good policy and to write good legislation which will be coming out of this committee. So that--that brings me to a follow up on my colleague Ms. Rice's questions about data. As she mentioned, and it's my understanding that all three of your platforms chose to remove content that was posted regarding the Capitol insurrection on January sixth.

And I think we can all understand some of the reasons for that, but as a result it's unavailable to researchers and to Congress. So my question for each of you is will you commit to sharing the removed content with Congress to inform our investigation of the events of January sixth and also the issues before us today about how to respond to extremists and dangerous content online? And I'll--I'll start with Mr. Zuckerberg.

ZUCKERBERG: Thanks, Congresswoman. When we take down content that might be connected to a crime I think we--we do as a standard practice try to maintain that so we can share with law enforcement if necessary. And--and--and I'm--I'm sure our team can follow up to discuss that with you as well.

FLETCHER: Sure. I appreciate that. And I understand that you have a legal obligation to cooperate with authorities and law enforcement in these cases and I think that, you know, what I'm talking about is--is also sharing it with us in Congress and I appreciate--I appreciate your response there. Mr. Dorsey.

DORSEY: We would like to do this, actually. We've--we've been thinking about a program for researchers to get access to actions that we had to take. But all of this is subject to local laws of course.

FLETCHER: Well and that might be something that we can help craft here. So I think that, you know, it is consistently something we've heard from researchers as well as a--as a real area of challenge in not having the data. So I appreciate that. And Mr. Pichai? Do you also agree?

PICHAJ: Congresswoman, sorry. I was muted. We are working with law enforcement. I'm happy to connect with your office and, you know, we cooperate as allowed by law while balancing the privacy of the people involved.

FLETCHER: Well thank you. So I--I appreciate all of your willingness to--to work with us and to assist Congress in addressing this attack on--on our Capitol and--and our country. Another idea that I would like to touch base with you on in the time I have left, just over a minute, is the difference we see in how your platforms handle foreign extremist content versus domestic content. And by all accounts your platforms do a better job of combatting posts and information from foreign terrorist organizations or FTOs like ISIS or al-Qaeda. And others where the posts are automatically removed depending on key words and phrases, et cetera.

The FTOs are designated by the State Department through a rigorous criteria to identify groups that wish to come--cause harm to Americans. Currently there is no legal mechanism or definition for doing the same for domestic terror and hate groups. Would a federal standard for defining a domestic terror organization similar to FTOs help your platforms better track and remove harmful content from your sites? Mr. Zuckerberg?

ZUCKERBERG: Congresswoman, I'm not sure. I think in--in domestically we do classify a number of white supremacist organizations and, you know, militias and conspiracy networks like Q-Anon as the--the same level of problematic as--as--as--as some of these other organizations then are able to take decisive action.

I think where this ends up being more complicated is--

FLETCHER: --I think--and I hate to cut you off but I'm gonna run short of time. So your answer was I'm not sure. Mi--can I just get a quick yes or no from Mr. Dorsey and Mr. Pichai?

DOYLE: Very quickly cause your time is expired. Very quickly.

DORSEY: We--we need to evaluate it. We need to understand what that means.

FLETCHER: Mr. Pichai.

PICHAH: Looking as--as domestic agencies focus on it I think we are happy to work and cooperate there.

FLETCHER: Thank you very much, Mr. Chairman. I yield back--

DOYLE: --Okay. The gentlelady's time is expired. It's my understanding we have, let's see, eight members who are requesting to waive on for the hearing. I believe we have given all members of the subcommittee their opportunity to speak so we'll now start to recognize the members waiving on. And first on the list here I see Mr. Burgess. Doc Burgess, are you with us?

BURGESS: Yeah, I am. Good--

DOYLE: --Okay. You're recognized for five minutes.

BURGESS: (INAUDIBLE). Tha--thank you--thank you, Mr. Chairman. And thanks to our--to our witnesses for spending so much time with us. And this is clearly a very important issue to every member of this committee regardless of which political party they identify with. I think--I guess, Mr. Zuckerberg, let me just ask you a question. Because it strikes me listening to your answers to both our colleague Jeff Duncan and our colleague Angie Craig, both coming at the issue from--from different directions.

But the concern is that there was a--there was the exercise of--of editorial authority over the postings that were made on--on--on your website. Is that a fair assessment?

ZUCKERBERG: Congressman, I'm not sure what you mean. But I think content moderation and forcing standards I--I don't think that that's the same kind of editorial judgment that for example a newspaper makes when writing a post.

BURGESS: Yeah, but maybe it is. Because Mr. Duncan eloquently pointed out there was restriction of conservative speech. And our colleague Angie Craig eloquently pointed out how there was restriction of--of trans-affirming speech. So that strikes me that the--we're getting awfully close to the line of exercising editorial discretion.

And forgive me for thinking that way, but if--if that is--and--and I'm sure I'm not alone in this. It does call into question then the immunity provided under Section 230. Maybe it is not the problem with the--the--the law itself, Section 230. Maybe the problem is that the mission has changed in--in your organization and other organizations.

ZUCKERBERG: Congressman, I'm not sure what you--what you mean but we have clear standards against things like terrorist content, child exploitation, incitement of violence, intellectual prop--property violations, pornography. Things that I would imagine that you agree with. And we--

BURGESS: --Also--

ZUCKERBERG: --Enforcement standards--

BURGESS: --All spelled out--all spelled out in the plain language of Section 230. And--but again, you're putting restrictions on conservative speech. Mr. Duncan eloquently pointed out how that is occurring. Angie Craig eloquently pointed out how you're putting restrictions on trans affirming speech. None of those fall into any of the

other categories that you're describing, so to the--just to the casual observer, it appears that you're exercising editorial authority. And as such, maybe you should be regulated as a publisher as opposed to simply someone who is carrying--who is indifferent to the content that they are carrying.

ZUCKERBERG: Congressman, I think one of the virtues of Section 230 is it allows companies to moderate things like bullying that are not always clearly illegal content, but that I think you and I would probably agree are harmful and--and bad. So I think it's important that companies have the ability to go beyond what is legally required.

I do not think that that makes these internet platforms the same thing, as you know, a news publisher who is literally writing the content themselves. You know, I do think we have more responsibility than maybe a telephone network where we're--

BURGESS: --Okay, let me let me interrupt you, in the interest of time, because I do--I want to pose the same question to Mr. Dorsey. Mr. Dorsey, every presidential tweet that I read, following the election had a--an editorial disclaimer appended to it by--by you. How does that not make you someone who's exercising editorial discretion on your--on the content that you're carrying?

DORSEY: Our goal with our labels was--was simply to provide connection to other data and provide context.

BURGESS: Yeah, but you don't do that routinely with--with other tweets. It seemed to be a singular assignment that someone had taken on to--to look at whatever the president is, is publishing. We're going to put our--our own spin on that. And that, again, that strikes me as an editorial exercise. And the only reason I bring this up--and--and, you know, we are going to have these discussions.

I recognize that smaller companies just starting out, the protection of Section 230 may be invaluable to them. But you all are no longer just starting out. You're established. You're mature companies. You exercise enormous, enormous control over the thought processes of not just an entire country, but literally an entire world.

You are exercising editorial discretion. I do think we need to revisit section 230 in the terms of have you now become actual publishers, as opposed to simply carriers of information. Thank you, Mr. Chairman. I'll yield back.

DOYLE: The gentleman yields back. The Chair recognizes Mr. Tonko for five minutes.

TONKO: Hey, thank you, Mr. Chair. Thank you for allowing me to waive on. Gentlemen, thank you for being with us today. While there are many issues I would like to raise with you, my most pressing unresolved questions revolve around and what I saw and experienced on January 6th when I had to dive for cover in the House gallery as violent insurrectionists attempted to break down the doors and take the chamber.

The rioters were breached the cap--who breached the Capitol Building were propelled by at least one belief, that the election had been stolen from former President Donald Trump. They reached the--this false and dangerous conclusion without evidence, yet, somehow in massive numbers. Their assault was not disorganized or isolated, and it was not coincidence.

So Mr. Zuckerberg, you and your colleagues have downplayed the role Facebook played in helping the writers mobilized on January 6th. In light of growing evidence that suggests otherwise, including the fact that Facebook was the most cited social media site in charging documents the Department of Justice filed against insurrectionists, do you still deny that your platform was used as a significant megaphone for the lies that fueled the insurrection?

ZUCKERBERG: Congressman, to be clear, I think part of the reason why we're--why our services are very cited in the charging docks is because we work closely with law enforcement to help identify the people who are there. So I don't view that--that collaboration with law enforcement should be seen as a negative reflection on our services.

And as I've said a number of times to today, there was content on--on our services from some of these folks. I think that that was problematic. But by and large, I--I also think that by putting in place policies banning QAnon, banning militias, banning other conspiracy networks, we generally made our services inhospitable to a lot of these folks and that had the unfortunate consequences of--of having those folks not use Facebook and use--and use other places as well. So there's certainly more for us to do. But I--I stand behind the work that we've done with law enforcement on this and--and the systems that we have in place.

TONKO: Thank you. Mr. Pichai, can you affirmatively state that YouTube did not recommend videos with Stop the Steal content, white supremacy content, and other hate and conspiracy content that were seen by riders at the Capitol?

PICHAU: Congressman, we had clear policies and we were vigorously enforcing the (INAUDIBLE). Just leading up to the election, we had removed hundreds of thousands of videos and we had terminated 8000 channels. And on the day of the riot, we were successfully able to take down inappropriate live streams. We gave precedence to journalistic organizations covering the event. And that's the content we raised up on YouTube that day. And since then, we have been cooperating with law enforcement as well.

TONKO: So you're--ou're indicating that you did not recommend videos with Stop the Steal?

PICHAU: We--we were rigorously enforcing--we have clear policies around content that undermined election integrity. Once the state certified the election on December 8th, we introduced a sensitive events policy. And we did take down videos, which were violative. And so we've been monitoring it very closely.

TONKO: And--thank you And Mr. Dorsey, are you confident that the conspiracy theorists or other purveyors of electoral this information and Stop the Steal on Twitter were not recommend it to others?

DORSEY: Not--I can't say that with confidence, but we--I know, we did work really hard to make sure that if we--if we saw any amplification that went against the terms of service, which this would, we took action immediately. We didn't have any upfront indication that this would happen, so we--we had to react to it quite quickly.

TONKO: All right. Thank you. So who and what content your platforms recommend have real world consequences and the riot caused five deaths and shook our democratic foundations. I believe that your platforms are responsible for the--for the content you promote and look forward to working with my colleagues to determine how to hold you accountable. Mr. Pichai and Google and YouTube often slip under the radar as a source of disinformation, but in the last election, bad actors used ads on Google Search to scam people looking for voting information. And YouTube failed to remove videos that spread misinformation about the 2020 vote results.

So Mr. Pichai, when journalists pointed out in November, that election misinformation was rampant on Google's YouTube, the company said it was allowing discussions of election processes and results. A month later, YouTube said it would remove new cont--content alleging widespread voter fraud in the 2020 election. Why did YouTube wait a month to take action on election misinformation?

PICHAU: If I could clarify here, we--we were taking down videos leading up to the election. We did--there is obviously a month from the date of election till there are due processes, co-challenges, and we waited till this--you know, we consulted with CSPA and the Association of Secretaries of State. And on December 8th, when the states certify the election, you know, we started enforcing newer policies on December 9th.

To be very clear, we were showing information from the Associated Press. And we were proactively showing information high up in our search results to give, you know, relevant information throughout--throughout this election cycle.

DOYLE: The gentleman's time has expired.

TONKO: Thank you. Mr. Chair, I yield back.

DOYLE: The Chair recognizes Mr. McKinley for five minutes.

MCKINLEY: Thank you, Mr. Chairman. And--and this--this panel, you all have to be exhausted after being grilled all day long like this. So my questions are to Mr. Zuckerberg. When you came before our committee in 2018, you acknowledged that Facebook had--had used what you just said clear standards preventing the sale of illegal drugs on your site. But you were shown--you were showing examples of active posts that traffickers were still using that platform unlawfully to sell prescription opioids.

Now, you--you did apologize and confirm that, quote, "Social media companies need to do a better job of policing these posts." Now, three years later, it appears a shell game is emerging. Facebook seems to have cleaned up its act, but you're now allowing Instagram one of your subsidiaries to become the new vehicle. Even though Instagram has--has the same policies against the sale of illegal substances, you're still allowing bad actors to push pills on your site. Look, it didn't take long for our staff to find numerous examples

[*]MCKINLEY: Here's oxycodone that--that was--is being sold on your site. Here's Ritalin that's being sold on your site. Here's Xanax; an Adderall that's being sold on your site. So I--these posts have--they're not new. They've been active since last fall. If we can find posts this easily, shame on you for not finding them for yourself.

Apparently, you're not taking the warnings of Congress seriously. After drug manufacturers dump millions of pills into our community, killing thousands ravaging families and destroying livelihoods, Congress responded by passing laws to hold them liable. If a retail store is selling cigarettes, or other--to underage kids, that store is held liable.

So why shouldn't you be held liable as well? Don't you--do think you're above the law? You're knowingly allowing this poison to be sold on your platform into our communities to our children to our vulnerable adults. Look, I've read Scott Galloway's, The Four. I encourage all the members on this committee to take--to read his book. It's a perfect depiction of the arrogance of Big Tech companies like Facebook, Google, Apple, and Amazon. He develops a very compelling argument as to why Big Tech companies should be broken into smaller companies, much like that occurred in AT&T in 1984.

Maybe it's time for Congress to have an adult conversation about this loss of liability protection and the need to reform our antitrust laws. I don't think Congress wants to tell you how to run your company, but maybe it should. So Mr. Zuckerberg let me--let me close this one question. And--so don't you think you'd find a way to stop these illegal sales on your platforms if you were held personally liable?

ZUCKERBERG: Keep on getting muted. Congressman, we don't want any of this content on our platforms. And I agree with you that this is a huge issue. We've devoted a lot of resources and a built systems that are largely quite effective at finding and removing the content. But I just think that what we all need to understand is that at the scale, that--that these communities operate, where people are, are sharing millions or, in messages, billions of things a day, it is inevitable that we will not find everything, just like a police force in a city will not stop every single crime. So I think that we should--

MCKINLEY: --I asked you the question very directly, Mark, (INAUDIBLE). Should you not be held liable when people are dying because your--your people are allowing these sales to take place? We did it with manufacturers. We do it in the stores. Why aren't we doing it to the salesman that allows us to take place?

ZUCKERBERG: Well, Congressman, I don't think we're allowing this to take place. We're--we're building systems that take the vast majority of this content off our systems. And what I'm saying--

MCKINLEY: --We've been dealing with this for three years, Mark. We've been doing--three years this has been going on. And you said you were going to take care of it last time, but all you do is switch from Facebook over to Instagram. They're still doing it now and you're saying we need to do more? Well, how many more families are going to die? How many more children going to be addicted while you still study the problem? I think you need to be held liable.

ZUCKERBERG: Congressman, we're not--we're not sitting and studying the problem. We're building effective systems that work across both Facebook and Instagram. But what I'm saying is that I don't think that we can expect that any platform will find every instance of harmful content. I think we should hold the platforms to be responsible for building generally effective systems at moderating these kinds of content.

DOYLE: The gentleman's time has expired--

MCKINLEY: --(INAUDIBLE) I'm not going to get an answer, Mike. Thank you.

DOYLE: The gentleman yields back. The Chair recognizes Ms. Blunt Rochester for five minutes.

BLUNT ROCHESTER: Thank you, Mr. Chairman, for allowing me to wave on to this important hearing. And thank you to the witnesses. I want to focus on two areas. First, consumer protection and safety issue. And second, more broadly, manipulation and privacy of our data.

On consumer protection and safety, earlier this year, two infants from two different families ended up in the intensive care unit in Wilmington, Delaware after being fed homemade baby formula based on instructional videos viewed on YouTube. One infant suffered from cardiac arrest that resulted in brain damage. For years, the American Academy of Pediatrics has warned parents against homemade baby formulas because it puts infants at risk of serious illness and even death. And since at least 2018, the FDA has recommended against the use of homemade formula. Even as recently as 29 days ago, the FDA issued an advisory against homemade formula.

In February, my office informed your team, Mr. Pichai, and as a follow-up I've sent a letter requesting information and action on this issue and hope--in the hopes of a response by April 1st. Mr. Pichai, this is just a yes or no question. Can I count on a response to my letter by the deadline of April 1st?

PICHAJ: Congresswoman, definitely yes; heartbreaking to hear the stories. We have clear policies. My understand--thanks for your highlighting--

BLUNT ROCHESTER: --Thank you--

PICHAJ: --This area. I think our--the videos have been taken down and we're happy to follow up and update with you.

BLUNT ROCHESTER: We--we--we checked today. For years, these videos have clearly violated your own stated policy of banning the videos that endanger the, as you say, "physical well-being of minors." And so, I'm--I'm pleased to hear that we will be hearing back from you.

And while we're considering Section 230, what's clear from this hearing is that we should all be concerned by all of your abilities to adequately and just as importantly rapidly moderate content. In some of these cases, we're talking life-and-death.

Second, as many of my colleagues have noted, your company's profit when users fall down the rabbit hole of disinformation. The spread of disinformation is an issue all of us grapple with from all across the political spectrum. Disinformation often finds its way to the people most susceptible to be--to it because the profiles that you create through massive data collection suggest what they would be receptive to.

I introduced the DETOUR Act to address common tactics that are used to get such personal data as possible. These tactics are all--often called dark patterns, and they are intentionally deceptive user interfaces that treat people into handing over their data. For the people at home, many of you may know this, as when you don't want to nap it doesn't allow you to have a no option or it will insinuate that you need to do something else, install another program like Facebook Messenger app to get on Facebook.

You all collect and use this information. Mr. Pichai, yes or no, would you oppose legislation that banned the use of intentionally manipulative design techniques that trick users into giving up their personal information?

PICHAJ: We definitely are happy to have oversight on these areas and explain what to do.

BLUNT ROCHESTER: Thank you. I have to go to Mr. Dorsey. Mr. Dorsey, yes or no?

DORSEY: Open to it.

BLUNT ROCHESTER: Mr. Zuckerberg?

ZUCKERBERG: Congresswoman, I--I think the principle makes sense.

BLUNT ROCHESTER: Yes or no, please?

ZUCKERBERG: And the details matter.

BLUNT ROCHESTER: Okay. Mr. Zuckerberg, your company recently conducted this massive ad campaign on how far the Internet has come in the last 25 years, great ad. You end it with the statement, "We support updated Internet regulations to address today's challenges." Unfortunately, the proposal that you direct your viewers to fails to address dark patterns, user manipulation, or deceptive design choices. Mr. Zuckerberg, will you commit now to include deceptive design choices as part of your platform for better Internet regulations?

ZUCKERBERG: Congresswoman, I'll--I'll--I'll think about it. My--my initial response is that I think that there are other areas that I think might be more urgently in need.

BLUNT ROCHESTER: That--that might be your--if you say this is a--a desire of yours to address the issues that we face today, dark patterns goes back to, you know, 2010, the--you know, this whole issue of deceptive practices. And I hope that you will look into it.

I--I will say--Ms. Trajan and others have mentioned--she mentioned our children. Others have mentioned seniors, veterans, people of color, even our very democracy is at stake here. We must act. And assure you, we will assure you we will act. Thank you so much. Mr. Chairman, I yield back six seconds.

DOYLE: I think the gentlelady. The gentlelady yields back, and now the chair recognizes Mr. Griffith for five minutes.

GRIFFITH: Thank you very much, Mr. Chair. According to new data from the National Center for Missing and Exploited Children's cyber tip line found that--that the vast majority of child exploitation reports were Big Tech sites. Facebook at the most, 20.3 million. Google was second with 546,000bplus. Twitter had 65,000 plus.

Put in perspective, MindGeek, the Canada-based parent company of major porn websites had 13,229. Facebook claims 90 percent of the flagged incidents were duplicates. All right, let's accept that. That still leaves over 2 million incidents, 2 million incidents. Mr. Zuckerberg, yes or no, does Facebook have a problem with child exploitation on its platform?

ZUCKERBERG: Congressman, this is an area that we work on a lot, but the reason why those numbers are so high is because we're so proactive about trying to find this and--and send it NCMEC and others who--who are doing good work in this area. We send--then content and flags over to them quite liberally whenever we think that we might see that something is an issue. And that's, I think, what the public should want us to do, not criticize us for sending over a large number of flags, but--but--but--but should encourage the companies to be doing this.

GRIFFITH: So, you're admitting that you all have a problem and you're--and you're--this is one way you're trying to work on it.

Mr. Pichai, yes or no, do you agree with Mr. Zuckerberg that you all have a problem? Are you there?

PICHAJ: Congressman, sorry, I was muted. This is an area in which we invest very heavily. We have been praised by several authorities. We work proactively.

GRIFFITH: So, the answer is yes. Mr. Dorsey, yes or no, do you agree?

DORSEY: If--if we see any problems, we try to resolve them as quickly as possible.

GRIFFITH: But you have problems, and that's why you're trying to resolve them. I--I get that. The problem is, when you're talking about millions of incidents, and we take 90 percent of them as duplicates from the Facebook data, that's millions of incidents that are happening where our children are being exploited with child pornography on you all's sites. We gotta do better.

I think you all need for everything we've talked about today an independent industrywide review team like electronic--the electronic industry did with the Underwriters Laboratory nearly 150 years ago. I told you all that when you're here before. Nobody's done anything. I don't think it needs to be within your company. I think it needs to be outside.

And--and on that vein, I would say to Google, special permission was given to Moonshot CVE to target ads against extremist keywords. Moonshot then directed thousands of individuals who search for violent content to videos and posts of a convicted felon who--who espouses anti-law enforcement, anti-Semitic, and archivist viewpoints. Mr. Pichai, are you aware of this problem?

PICHAJ: Congressman, I'm not aware of this specific issue. Last year, we blocked over 3.1 billion bad acts, 6000 acts per minute. And so, we enforce vigorously, but I'm happy to look into this specific issue and follow-up back with you.

GRIFFITH: Well, here's what happened. You partnered with an outside group that didn't do their job. What are your standards when you partner with an outside group? What are your standards and what are your philosophy? Because they sent people who are already looking for violence to an--a convicted felon with anarchist and anti-Semitic views.

PICHAJ: There is no place for hate speech. And, you know, I--I'm disappointed to hear of this. We will definitely look into it and follow back with you.

GRIFFITH: Well, and I appreciate that--I--I recognize that. But I have the same concerns that Mr. McKinley had. And you weren't here last time, but we heard the same kinds of things about how we're going to work on it and how we're going to get these problems resolved. And I forget when that hearing was, but a year so ago. And yet we continue to have the same problems where political candidates' information is being taken down because for some reason it's--it's flagged, where conservatives and people on the left are being hit and taken down.

I agree with many of the sentiments on both sides of the aisle that if--if--if you all aren't doing anything and it appears that you're not moving fast enough, we have no choice in Congress but to take action. I don't want to. I'd rather see you all do it like the electric industry did with Underwriters Laboratory. But nobody's doing that.

Nobody's coming up with a group that both sides of the aisle and the American families can fill comfortable with.

And so, we're going to have to take action, and is probably going to be this year. I yield back.

DOYLE: The gentleman yields back. The chair recognizes Ms. Schrier for five minutes.

SCHRIER: Thank you, Mr. Chairman. I'm a pediatrician and I have spent my life calming patients who are nervous about vaccines because of online disinformation. In fact, that's why introduced the Vaccines Act when I was a new member of Congress. Did you know that there are doctors who, after spending their entire day on the front line fighting this virus, they come home at night and spend their scarce free time and family time fighting misinformation on vaccines online? And this information, of course, comes primarily from Facebook and Twitter.

So, the question is why do they do that. Well, they do it because of things like this that happened after I introduced the Vaccines Act. Here are some overt threats. "Keep shoving this vaccine mantra down people's throats and expect riots." "Be careful, you will answer for this tyranny one day." "She needs to just disappear. Can we vote her out of office?" "I'm enraged over these poison pushers. We have weapons and are trained to fight off possible forced vaccinations. I will die protecting my family."

And then there's just the misinformation. "It says safe and effective many times, yet no vaccine has been studied in a double-blind study." False. "Who's going to take this vaccine? I heard rumors that it changes a person's DNA." False. "You do not give--excuse my language, "You do not give a shit about the health and welfare of our children. This horrid vaccine has already killed 600 people. You're deplorable." And of course, that again is false.

So, while the overt threats are unsettling, particularly after January 6th, I think about this whole ecosystem, your ecosystem that directs a hostile sliver of society en mass to my official Facebook page. And these are not my constituents. In fact, most came from two specific groups that directed their members to my page.

Mr. Zuckerberg, I have some questions for you. I know you understand these issues are important, and sometimes misinformation can be very hard to spot. Would you agree?

ZUCKERBERG: Congresswoman, I agree with both of those. This is important and--and the enforcement processes can be difficult.

SCHRIER: Thank you. And I heard your answer earlier to Representative Upton's question that there are 35,000 people doing content review of posts that have been flagged by users and AI. Can you tell me what content review means and how many of those 35,000 are dedicated to topics regarding health?

ZUCKERBERG: Congresswoman, yes, what--what the people are doing overall is, you know, content gets flagged either by the AI systems or by another person in the community. And if the AI can't by itself determine that something there violates or doesn't, then it gets flagged for--for a human review and human judgment, and the 35,000 people go through all those different queues focused on all of the different types of harms that we've discussed today.

I don't have the number off the top of my head about how many of them are focused on vaccine misinformation. But as you know, we have a policy that doesn't allow vaccine misinformation, and we work with the WHO and CDC to take down false claims around COVID and--and the vaccines around that that could cause harm.

SCHRIER: That's where really gets tricky because you have to have experts and healthcare professionals who really understand. Are they--are your people trained in healthcare to really even be able to discern what's real, what's fake, and what to take down?

ZUCKERBERG: Congresswoman, the people who set the policies either are experts in these areas or engage in a consultative process where they talk to a lot of these different folks. In this case, we largely refer to the CDC and WHO on which claims they think are going to be harmful, and that we try to break that down into kind of very simple protocols that the 35,000 people follow and that we can build into AI systems to go find as much of that content proactively as possible without requiring all those people to be medical experts.

SCHRIER: So, with my short time remaining, I would love to jump to that part about--about the CDC, because I want to turn my attention to the--the COVID resource center that you describe as a central part of your efforts to fight misinformation. You directed over 2 billion people to the COVID-19 information center.

But on that information page, almost all of the content links to additional Facebook pages. It looks to me like an extension of Facebook's walled garden that just keeps users on the site instead of leading directly to authoritative trusted sources like the CDC. So, knowing that your platform is a large source of misinformation, did you consider just referring people directly to sites like the CDC rather than keeping them within your platform?

ZUCKERBERG: Congresswoman, I—I think we have considered both, and I think we have done both in different cases. I—I—the team is—is very focused on—on building this in a way that is going to be most effective at getting people to actually see the content and I—I believe that they've concluded that showing content from people who—within a—a person's community that they are going to trust on the services is one of the most effective things that we can do.

DOYLE: Gentlelady's time is expired.

SCHRIER: Thank you. I yield back.

DOYLE: The Chair now recognizes Mr. Crenshaw for five minutes.

CRENSHAW: Thank you, Mr. Chairman. Thank you all for being here. It's been a long one. I've been on social media longer than anyone in Congress I think. I was one of the first schools to have Facebook back in 2004. And it seemed to me that the goal of social media was simply to connect people. Now the reason we are here today is because the role of social media has expanded in an extraordinary way and your power to sway opinions and control narratives is far greater than the U.S. government's power ever has been.

So I noticed a trend today—there's a growing desire from many of my colleagues to make you the arbiters of truth. See they know you have this power and they want to direct that power for their own political gain. Mr. Zuckerberg, since Facebook was my first love, I'm going to direct questions at you—and this isn't a trick question, I promise—do you believe in the spirit of the 1st Amendment, free speech, robust debate—basic liberal values?

ZUCKERBERG: Yes, absolutely.

CRENSHAW: See, my colleagues can't infringe on the 1st Amendment. The American people in your speech are protected from government as they should be. My colleagues, this administration they can't silence people they disagree with no matter how much they want to. But I do think they want to. Just in this hearing I've heard Democrats complain about misinformation by which they clearly mean political speech they disagree with. The complaint today that Prager University content is still up. I've heard them accuse conservative veterans of being tinfoil hat-wearing extremists and that opinions on climate change that they disagree with should be taken down. This is quite different from the Republican complaint that illegal content needs to be addressed.

There is a growing number of people in this country that don't believe in the liberal values of free speech and free debate. I promise you the death of the 1st Amendment will come when the culture no longer believes in it. When that happens, it becomes OK to jail or investigate citizens for speech like has happened in Canada and throughout Europe. Their culture turned against free speech. You all sitting here today as witnesses are part of the culture. You can stand up for the spirit of open debate and free speech or you can be the enemy of it.

Your stance is important because it's clear that many want to weaponize your platforms to get you to do their bidding for them. Mr. Zuckerberg, do you think it's your place to be the judge of what is true when it comes to political opinions?

ZUCKERBERG: Congressman, no. I don't believe that we should be the arbiter of truth.

CRENSHAW: Thank you. And look, I promise you this—as long as you resist these increasing calls from politicians to do their political bidding for them I will have your back. You don't, you become an enemy of liberty in longstanding American tradition. You might all agree in principle with what I just said, Mr. Zuckerberg, you clearly do and I appreciate—I have a feeling the others would answer it as well I just don't have time to ask everybody. But the fact remains that community standards on social media platforms are perceived to be applied unequally and with blatant bias. Mr. Dorsey, in just one example I saw a video of from Project Veritas that was taken down because they confronted a Facebook executive on his front lawn.

Here's the thing—I can show you a video of CNN doing the exact same thing to an old woman who was a Trump supporter in her front yard. I've looked at both videos—it's an apples to apples comparison. CNN remains up. Project Veritas was taken down. I'll give you a chance to respond to that. I have a feeling you're going to tell me you have to look into it.

DORSEY: I--I don't have an understanding of the--of the case but I would imagine if we were to take a video of that down it would be due to a doxing concern. Whatever that is.

CRENSHAW: The address was blurred out. I look at you don't have the--you don't have the case in front of you, I get that. The point is if there is countless examples like this I just asked, I just found that one today. There's countless examples like this. So even if we agree in principle and everything I just went over you guys have lost trust. And you've lost trust because this bias is seeping through. We need more transparency. We need better appeals process. And more equitable application of your community guidelines because we have to root out political bias in these platforms.

I--I think and I talked with a lot of you offline or at least your--your staff and I think there is some agreement there and I haven't heard in this hearing anybody ask you what you're doing to--to--to achieve these goals. So I will allow you to do that now. Maybe, Mr. Zuckerberg, we'll start with you.

ZUCKERBERG: Sorry, to achieve which goals?

CRENSHAW: More transparency, more--more feeling better appeals process for content taken down, more equitable application of community guidelines.

ZUCKERBERG: So, for transparency we issue quarterly community standards enforcement reports on how like what prevalence of harmful content of each category from their terrorism to incitement of violence to child exploitation all the things that we've talked about. How much of it there is and how effective we are at--at finding that and stats around that.

For appeal, the biggest thing that we've done is set up this independent oversight board which is staffed with people who all have a strong commitment to free expression for whom people in our community can ultimately appeal to them and that group will make a binding decision including overturning several of the things that we have taken down and telling us that we have to take them--that we have to put them back up and then we respect that.

DOYLE: Gentleman's time is expired. Chair now recognizes last but not least, my fellow Pennsylvanian, Mr. Joyce, you're recognized for five minutes.

JOYCE: Thank you for yielding. And thank you Mr. Chairman and the ranking members for convening this hearing. I thank you all. It's been a long day. But this is an incredibly important day. We have heard consistently during this hearing about alarming accounts of content policing, censorship and even permanent de-platforming of individuals. I've also been concerned about the lack of transparencies and consistent in Facebook's application of Facebook's owns standards. As you mentioned, I'm a representative from Pennsylvania. And in my district Facebook shut down the personal pages of Walt Dehosky(PH) and Charlotte Schaffer(PH) as well as the Adams County Republican Committee Facebook page that they administered in historic Gettysburg, Pennsylvania. And this all occurred without warning.

Since ethe pages were taken down in December, these Pennsylvanians haven't received an acceptable answer from Facebook about why there were banned nor have they been given the opportunity to appeal this decision.

Mr. Zuckerberg, could you please explain how something like this could happen?

ZUCKERBERG: Congressman, I'm not familiar with those specific details but in general, I agree that building out a better appeals process and better and more transparent communication to people about why specific decisions were made is one of the most important things that we need to do next. And--and that's one of the big things on our road map for--for this year and next year and I--and I hope we can dramatically improve those experiences.

JOYCE: Mr. Zuckerberg, may I get from you a commitment that a more concise and transparent appeals process will be developed?

ZUCKERBERG: Congressman, yes. We're working on--on more transparent communication to people and--and more of an appeals process as part of our product roadmap now as I just said.

JOYCE: And will you commit to getting my constituents answers as to why they were banned?

ZUCKERBERG: Congressman, I can certainly have my team follow up with them and--and--and make sure that we can--we can do that.

JOYCE: Thank you for that--I am also concerned by potential partisan bias in Facebook's enforcement of its content policies. Shutting down the Adams County Republican Committee Facebook page strikes me as an infringement on speech and that is normally protected in the public domain. Mr. Zuckerberg, does Facebook maintain data on how many Democrat and Republican county committee pages that you have banned from your platform?

ZUCKERBERG: No, Congressman, we don't--we don't generally keep any data on--on the--on whether the people who use our platform are Democrats or Republicans so it's hard for us to (INAUDIBLE).

JOYCE: My time is running short here and it's a long day--but Mr. Zuckerberg you say you have not maintained that data--would you consider gathering such data to verify that there is no political bias in your enforcement algorithms?

ZUCKERBERG: Congressman, I'm not sure that that's a--that that's a great idea and that--I don't know that most people would want us to collect data on whether they're a Democrat or a Republican and have that be a part of our--our overall system.

JOYCE: I think there's a huge disparity as I represent Pennsylvania and I think that data would be appreciated if shared with us in a fair manner. My next question is to Mr. Dorsey--does Twitter maintain data on the political affiliations of (INAUDIBLE) accounts that you block?

DORSEY: No.

JOYCE: Have you determined that any political bias is necessary for your enforcement?

DORSEY: Not sure what you mean, but no.

JOYCE: I think that these discussions today are so important. I think that you all recognize that the platforms that you represent have developed an incredible ability for Americans to connect and contact. But these free speech that we hold so dear to us must be maintained. Again, I thank the Chairman. I thank the ranking member for bringing this together and allowing us to present what I feel our sincere concerns to you. Thank you, Mr. Chairman, and I yield.

DOYLE: I thank the gentleman. The gentleman yields back. Everyone who wanted to ask the question has asked one, and I want to thank all of you for your patience today. I request unanimous consent to enter the following records, testimony, and other information into the record.

A letter from Asian Americans Advancing Justice; a letter from the Leadership Conference on Civil and Human Rights; a letter from New America's Open Technology Institute; a letter from New York Small Pharma Limited; a statement from the Alphabet Workers Union; letters from National Black Jacks--Justice Coalition; a letter from Sikhs for Justice; a letter from State AGs; a letter from the Computer and Communications Industry Association; a letter from AVAAZ; opening statement from Anna Eshoo; a blog from Neil Fried of Digital Frontiers Advocacy; a letter from the Music Community; a letter from the Disinfo Defense League; a letter from Consumer Reports; a report from the Center for Countering Digital Hate called the Disinformation Dozen; a letter from the Coalition for a Secure and Transparent Internet; a letter from the Sikh American Legal Defense and Education Fund; a letter from Gun Violence Survivors; Faces of Tech Harm Congress; a letter to YouTube from Rep. Eshoo; a letter to Facebook from Rep. Eshoo; a letter to Twitter from Rep. Eshoo; a longitudinal analysis of YouTube's promotion of conspiracy bids--video--conspiracy videos; a letter from the Alliance for Safe Online Pharmacies; a CCIA statement; a comment by Donovan et al from the Technology and Social Change Team; a Wall Street Journal article titled Facebook Executives Shut Down Efforts to make site less divisive; a Voice of America article titled FBI Surge and Internet Crime Cost Americans \$4.2 billion; a Global Research Project Report; an opinion article titled Google is not Cracking Down on the Most Dangerous Drug in America; an MIT Technology Review article titled How Facebook got Addicted to Spreading Misinformation, an article from the Independent; an article from the New Yorker; a letter from the Coalition of Safer Web; a New York Times article titled Tech Companies Detect a Surge in Online Videos of Child Sex Abuse; an MIT review article titled Thank You for Posting: Smokers Lessons for Regulating Smoke--Social Media; an article from In primis; an article from the Atlantic; a New York Times article titled Square: Jack Dorsey's Pay Service is Withholding Money Merchants Say They Need; a response letter from Twitter to Rep. Rogers; a response letter from Google to Rep. Rogers; a response letter from Facebook to Rep. Rogers; an article from an get--Engadget; a letter regarding Spanish-language misinformation; data from the

Centers for Disease Control, the National Survey on Drug Use and Health, and the Mercado, Hollen (PH), Lima (PH), Stone and Wang regarding teen mental health; a report from the House Committee on Veterans Affairs. Without objection, so ordered.

I want to thank our witnesses today for appearing. We appreciate it. We appreciate your patience while you answered these questions from all members. I—I hope you can take away from this hearing how serious we are on both sides of the aisle to see many of these issues that trouble Americans addressed. But thank you for being here today. I want to remind all members that, pursuant to committee rules, they have 10 business days to submit additional questions for the records to be answered by the witnesses who have appeared. And I would ask that each witness to respond promptly to any questions that you may receive. At this time, this hearing is adjourned.

Copyright

Copyright 2021 CQ-Roll Call, Inc. All Rights Reserved.

DEFENDANTS' EXHIBIT 171:

INTENTIONALLY LEFT BLANK

DEFENDANTS' EXHIBIT 172:

INTENTIONALLY LEFT BLANK

DEFENDANTS' EXHIBIT 173:

Reaching Billions of People With COVID-19 Vaccine Information

[about fb.com/new/2021/02/reaching-billion-of-people-with-covid-19-vaccine-information/](https://about.fb.com/new/2021/02/reaching-billion-of-people-with-covid-19-vaccine-information/)

April 22, 2022



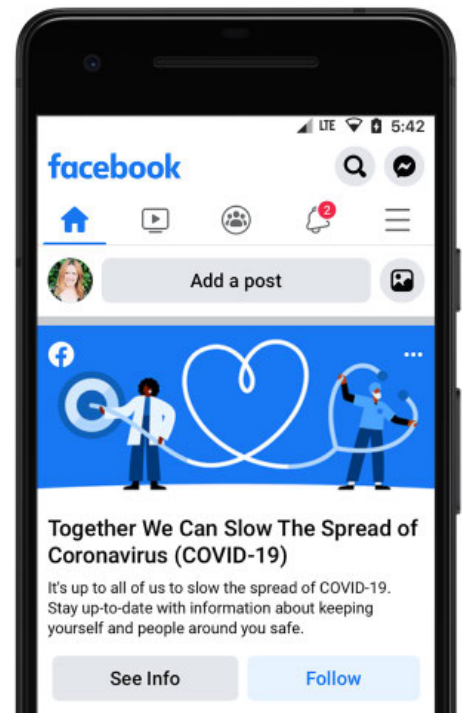
We're running the largest worldwide campaign to promote authoritative information about COVID-19 vaccines by:

- Helping people find where and when they can get vaccinated — similar to how we helped people find information about how to vote during elections
- Giving \$120 million in ad credits to help health ministries, NGOs and UN agencies reach billions of people around the world with COVID-19 vaccine and preventive health information
- Expanding our efforts to remove false claims on Facebook and Instagram about COVID 19 and vaccines
- Providing data to inform effective vaccine delivery and educational efforts to build trust in COVID-19 vaccines

A year ago, COVID-19 was declared a public health emergency and since then, we've helped health authorities reach billions of people with accurate information and supported health and economic relief efforts. We've connected over 2 billion people from 189 countries to reliable information about the coronavirus through our COVID-19 Information Center and informational messages, and we've removed more than 12 million pieces of content on

Facebook and Instagram containing misinformation that could lead to imminent physical harm. We've partnered with governments in more than 120 countries, as well as multilateral organizations like the World Health Organization (WHO) and UNICEF, to deliver timely information about COVID-19, including through helplines on WhatsApp.

2B+ people
from 189 countries
have been connected
to reliable information
about the coronavirus
through our COVID-19
Information Center



We've provided researchers and public health officials with real-time data and tools to help inform disease forecasting and understand the effectiveness of prevention measures. Through our Data for Good program, we've partnered with over 450 organizations in nearly 70 countries, the vast majority of which are leveraging our tools to support the COVID-19 response in their communities. And our publicly available datasets were downloaded over a million times in the last year by nonprofits, public health officials and researchers.

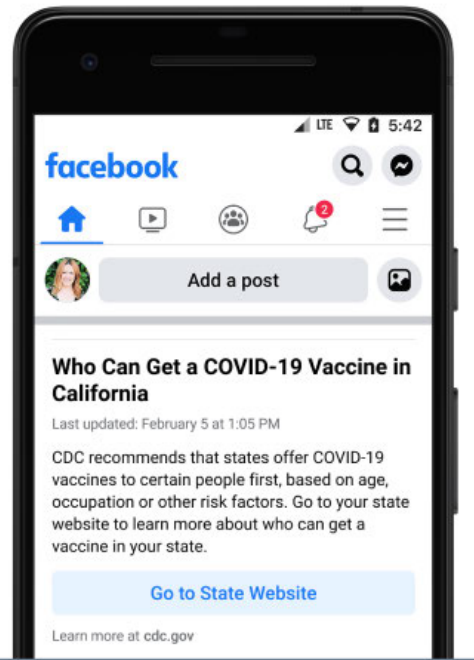
But there's still a long road ahead, and in 2021 we're focused on supporting health leaders and public officials in their work to vaccinate billions of people against COVID 19. Building trust and confidence in these vaccines is critical, so we're launching the largest worldwide campaign to help public health organizations share accurate information about COVID 19 vaccines and encourage people to get vaccinated as vaccines become available to them.

Helping People Find Where and When They Can Get Vaccinated

As public officials roll out information on COVID-19 vaccine availability, we'll help people find where and when they can get vaccinated—similar to how we helped people find information about where and when to vote during elections. Starting this week in the US, we'll feature

links in the COVID-19 Information Center to local ministry of health websites to help people understand whether they're eligible to get vaccinated and how to do so. And in the coming weeks, as more information becomes available, we'll continue to expand this feature to more countries and improve it to make it easier for people to see where and when they can get vaccinated in just a few taps.

As public officials roll out information on COVID-19 vaccine availability, we'll help people find where and when they can get vaccinated



Sharing Credible Information About COVID-19 Vaccines

We're working with health organizations and community leaders to run campaigns on our platform promoting accurate information about COVID-19 vaccines and encouraging people to get vaccinated. We're giving \$120 million in ad credits to help health ministries, NGOs and UN agencies reach billions of people around the world with COVID 19 vaccine and preventive health information. And we're providing training and marketing support to help governments and health organizations move quickly and reach the right people with the latest vaccine information.

\$120 million

given in ad credits to health ministries,
NGOs and UN agencies around the world

We'll soon bring the COVID 19 Information Center to Instagram so people can access the latest information about COVID-19 vaccines across our apps. We're also helping health authorities and governments share timely vaccine information over WhatsApp and provide answers to people's questions. We partnered with the government in Indonesia to create a helpline on WhatsApp that shares information on vaccine availability first with medical workers, and eventually with the general public. In just 5 days, 500,000 medical workers out of 1.3 million in the country — accessed the service. Other governments and health authorities, including the South Africa government and the WHO, are starting to create similar helplines to provide the latest vaccine information.

We're also working to amplify content that directly serves communities where vaccine intent and access may be lower. In the US, we're partnering with the Johns Hopkins Bloomberg School of Public Health to reach Native American communities, Black communities and Latinx communities, among others, with science and evidence-based content that addresses the questions and concerns these communities have. We're also working with AARP to reach Americans over 50 with educational content about COVID-19 vaccines, including Spanish language content designed to reach Latinx and Hispanic communities.

This builds on the work we've done with health organizations over the past year to increase adoption of COVID-19 preventive behaviors, such as wearing a mask. We put reminders at the top of Facebook and Instagram to wear a mask. And we reached over 26 million people with our public figure campaign encouraging people to #WearAMask, resulting in a 7-point increase in people reporting that wearing a mask in public is very or extremely important. We'll use insights and best practices from this work to inform vaccine information campaigns and support health authorities in building confidence in COVID-19 vaccines.

Combating Vaccine Misinformation

In addition to sharing reliable information, we are expanding our efforts to remove false claims on Facebook and Instagram about COVID-19, COVID-19 vaccines and vaccines in general during the pandemic. Today, following consultations with leading health

organizations, including the WHO, we're expanding the list of false claims we will remove to include additional debunked claims about COVID 19 and vaccines. Learn more about how we're [combating COVID-19 and vaccine misinformation](#).

We're expanding our efforts to remove false claims on Facebook and Instagram about COVID-19 and vaccines

Providing Data to Inform Effective Vaccine Delivery

Last year, we began collaborating with Carnegie Mellon University Delphi Research Group and the University of Maryland on COVID-19 surveys about symptoms people are experiencing, mask wearing behaviors and access to care. These surveys are conducted by our academic partners and Facebook does not receive individual survey responses. With over 50 million responses to date, the survey program is one of the largest ever conducted and has helped health researchers better monitor and forecast the spread of COVID 19. It's also the only source of global data on mask wearing, which has helped public health officials around the world in their COVID-19 response efforts. The Institute of Health Metrics and Evaluation used insights from the surveys to inform several mask mandates in countries such as Poland, which achieved a significant increase in mask wearing.

The survey data shows that people's willingness to get a COVID 19 vaccine varies widely across the world, with over 90% of people in Denmark saying they would take a COVID-19 vaccine compared to 71% in Argentina and 62% in the Philippines. And in the US, less than 60% of Black or African American people reported they would be likely to get a COVID-19 vaccine. So to help guide the effective delivery of COVID-19 vaccines, the survey data will provide a better understanding of [trends in vaccine intent](#) across sociodemographics, race, geography and more. The scale of the survey will also allow for faster updates on changes in trends, such as whether vaccine intent is going up or down in California in a given week and better insights on how vaccine intent varies at a local level. We'll share these new insights including [vaccine attitudes at a county level](#) in the US as well as [globally](#).

Data has proved critical in informing the fight against COVID 19. In 2020, we launched new datasets, maps and tools to support researchers, nonprofits and governments in their COVID-19 response, and in 2021, we'll continue to provide helpful data and insights to

understand vaccine attitudes, build trust in vaccines through reliable information and support vaccination efforts.

For more information about how we're providing data to aid in the fight against COVID-19, check out our [2020 Data for Good Annual Report](#). And to learn more about how we're supporting COVID-19 relief efforts and keeping people informed, visit our [COVID-19 action page](#).

DEFENDANTS' EXHIBIT 174:

From: Todd O'Boyle [toboyle@twitter.com]
Sent: 2/26/2021 1:15:11 AM
To: Qureshi, Hoor EOP/WHO [Hoor.Qureshi@who.eop.gov]
CC: Flaherty, Robert EOP/WHO [Robert.Flaherty@who.eop.gov]; Wakana, Benjamin L EOP/WHO [Benjamin.L.Wakana@who.eop.gov]; Humphrey, Clarke EOP/WHO [Clarke.Humphrey@who.eop.gov]; Lauren Culbertson [lculbertson@twitter.com]; Rowe, Courtney M. EOP/WHO [Courtney.M.Rowe@who.eop.gov]; Joshua Peck [joshua.peck@hhs.gov]
Subject: Re: [EXTERNAL] Checking in: Twitter meeting

Thanks so much, looking forward to it.
 Best,
 TO

On Thu, Feb 25, 2021 at 8:13 PM Qureshi, Hoor EOP/WHO <Hoor.Qureshi@who.eop.gov> wrote:
 2pm ET works great on our end. Just sent around a calendar invite for this!

From: Todd O'Boyle <toboyle@twitter.com>
Sent: Thursday, February 25, 2021 8:08 PM
To: Flaherty, Robert EOP/WHO <Robert.Flaherty@who.eop.gov>
Cc: Wakana, Benjamin L. EOP/WHO <Benjamin.L.Wakana@who.eop.gov>; Humphrey, Clarke EOP/WHO <Clarke.Humphrey@who.eop.gov>; Lauren Culbertson <lculbertson@twitter.com>; Rowe, Courtney M. EOP/WHO <Courtney.M.Rowe@who.eop.gov>; Qureshi, Hoor EOP/WHO <Hoor.Qureshi@who.eop.gov>; Joshua Peck <joshua.peck@hhs.gov>
Subject: Re: [EXTERNAL] Checking in: Twitter meeting

Hi Robert -
 How about 10am or 2pm (our preference) on Monday 3/1?
 Best.
 TO

On Thu, Feb 25, 2021 at 8:01 PM Flaherty, Robert EOP/WHO <Robert.Flaherty@who.eop.gov> wrote:
 Hey Todd — yes. Can you share some times that work on Monday? Our colleague Hoor can land a time for us.

Sent from my iPhone

On Feb 25, 2021, at 7:54 PM, Todd O'Boyle <toboyle@twitter.com> wrote:

Hi all -
 We are still interested in sharing an update with you on our work to address covid misinformation while also ensuring the reliable availability of quality information.

Recognizing that a meeting did not quite come together this week, are there a few times next week that would work for you?

Thank you very much,
Todd O'Boyle

On Thu, Feb 18, 2021 at 3:58 PM Wakana, Benjamin L. EOP/WHO <Benjamin.L.Wakana@who.eop.gov> wrote:

Adding a few others here.

From: Todd O'Boyle <toboyle@twitter.com>
Sent: Thursday, February 18, 2021 3:52 PM
To: Wakana, Benjamin L. EOP/WHO <Benjamin.L.Wakana@who.eop.gov>; Humphrey, Clarke EOP/WHO <Clarke.Humphrey@who.eop.gov>
Cc: Lauren Culbertson <lculbertson@twitter.com>
Subject: [EXTERNAL] Re: Transition <> Twitter meeting

Theo - Thank you for the prompt response. Moving you to bcc.

Ben and Clarke - The Twitter Policy team would like to share an update on our work to combat covid misinformation while also sharing reliable covid information. Do you have time to meet early next week? Perhaps Tuesday afternoon at 1 or 230? Otherwise we are happy to look at other times.

Thank you in advance.
Todd O'Boyle

On Thu, Feb 18, 2021 at 3:45 PM Theo LeCompte <tlecompte@jbrpt.org> wrote:

Hey Todd:

I'm about to roll off, but Ben and Clarke would be the folks to connect with on this.

Thanks!
Theo

On Thu, Feb 18, 2021 at 3:34 PM Todd O'Boyle <toboyle@twitter.com> wrote:

Gentlemen -

We would like to update you on some additional measure Twitter taking regarding covid. Do you have time on Tuesday afternoon of next week?

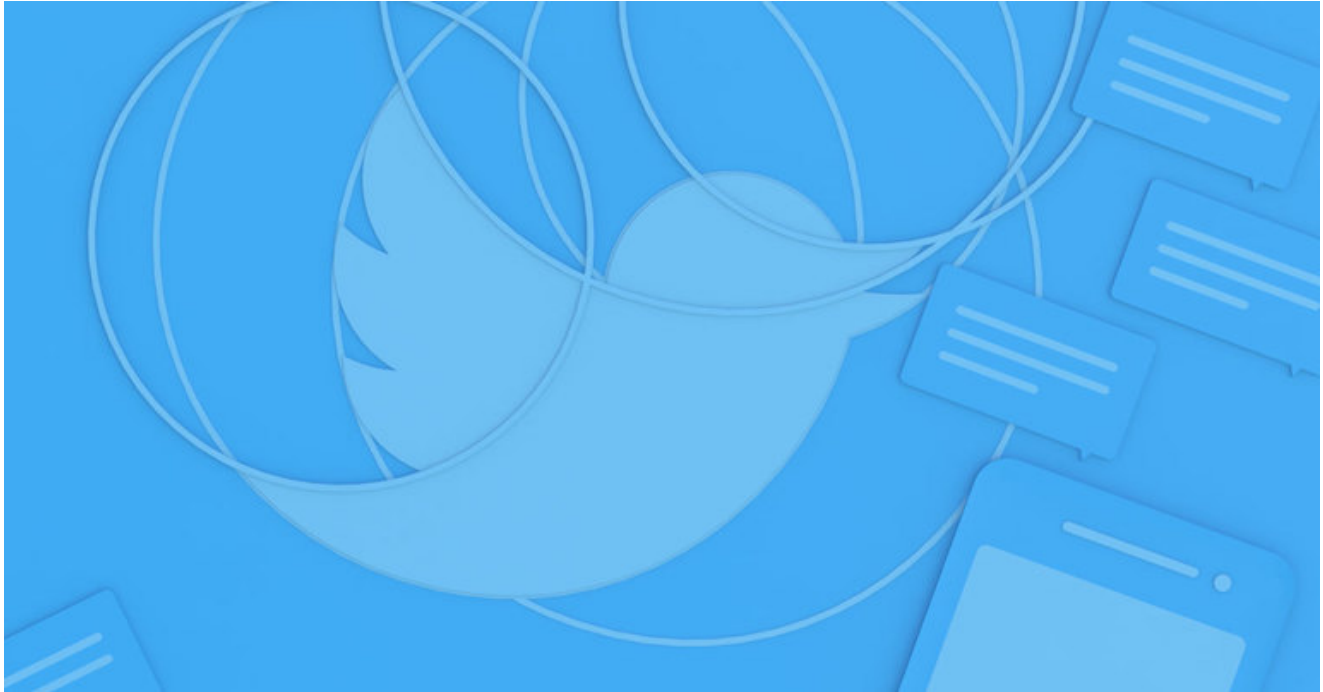
Are you two still the appropriate contacts? If not, please feel free to point me in another direction.
TO

.....
.....
.....
.....
.....

DEFENDANTS' EXHIBIT 175:

Updates to our work on COVID-19 vaccine misinformation

 blog.twitter.com/en_us/topic/company/2021/update_to_our_work_on_covid_19_vaccine_misinformation



Effective November 23, 2022, Twitter is no longer enforcing the COVID-19 misleading information policy.

This Tweet is unavailable



This Tweet is unavailable.

As the distribution of COVID-19 vaccines expands, people continue to turn to Twitter to discuss what's happening and find the latest authoritative public health information.

In December, we shared updates on our work to protect the public conversation surrounding COVID 19. Starting today, we will begin applying labels to Tweets that may contain misleading information about COVID-19 vaccines, in addition to our continued efforts to remove the most harmful COVID-19 misleading information from the service. Since introducing our COVID-19 guidance, we have removed more than 8,400 Tweets and challenged 11.5 million accounts worldwide.

We are also introducing a strike system that determines when further enforcement action is necessary. We believe the strike system will help to educate the public on our policies and further reduce the spread of potentially harmful and misleading information on Twitter, particularly for repeated moderate and high-severity violations of our rules.

This Tweet is unavailable



This Tweet is unavailable.

Example of COVID 19 misinformation label

Enforcement details:

Labels will first be applied by our team members when they determine content violates our policy. Those assessments will be used to further inform our automated tools and to advance our proactive capacity to identify and label similar content across the service. Our goal is to eventually use both automated and human review to address content that violates our COVID-19 vaccine misinformation rules. Machine-learning and automated language processing takes time to be effective. As such, we will begin with English-language content first and use this same process as we work to expand to other languages and cultural contexts over time.

Labels will appear in your set display language and may link to curated content and official public health information or the Twitter Rules. Our goal with these product interventions is to provide people with additional context and authoritative information about COVID-19.

Through the use of the strike system, we hope to educate people on why certain content breaks our rules so they have the opportunity to further consider their behavior and their impact on the public conversation. This strike system is similar to our recent update to the Civic Integrity Policy. Individuals will be notified directly when a label or required Tweet removal results in additional account-level enforcement. Repeated violations of the COVID-19 policy are enforced against on the basis of the number of strikes an account has accrued for violations of the policy.

- One strike: no account level action
- Two strikes: 12-hour account lock
- Three strikes: 12-hour account lock
- Four strikes: 7-day account lock
- Five or more strikes: permanent suspension

As always, if you believe that your account was locked or suspended in error, you can submit an appeal.

This Tweet is unavailable



This Tweet is unavailable

Example of COVID-19 misinformation label with engagements limited

Partnerships:

We are not only focused on enforcing the Twitter Rules, but also helping people find credible health information and partnering with the experts. We continue to work in close consultation with local, national, and global public health authorities around the world, most recently:

- **Finding reliable information.** Since January 2020, we have had a dedicated COVID-19 search prompt feature in place within the product. This means when someone searches for COVID-19, they are met with credible, authoritative content at the very top of their search experience. This has been expanded to over 80 countries worldwide and is currently available in 29 languages. In some countries the prompts now also include an additional button which links to COVID-19 vaccine specific information.
- **Pro bono advertising.** Through our Ads for Good grants, we continue to partner with nonprofits and NGOs around the world to elevate authoritative information on COVID-19. Throughout the pandemic we've supported these efforts across more than 35 countries on a pro bono basis. In addition, we have donated premium advertising products, including Promoted Trend and First View products, to elevate critical public health information such as @FEMA's message about the agency's vaccination efforts and emergency relief locations during winter storms.
- **Global cooperation.** In February 2021, we participated in a global WHO policy consultation to present Twitter's views on finding and implementing "innovative ways and best practices to address health misinformation in the social media sector." We continue to host a weekly live Q&A event page for the WHO at #AskWHO.
- **Addressing public questions on Twitter.** This month, we facilitated a Twitter Q&A from @WHCOVIDResponse. The Q&A featured Dr. Anthony Fauci, US President Biden's chief medical advisor, and other members of the White House COVID-19 response team. In India, we worked with the Ministry of Health to organize Vaccine Vartha, a weekly expert talk hosted on Twitter that enables vaccine experts to answer citizen questions.
- **Encouraging healthy conversation.** In January, in partnership with Team Halo, UNICEF, NHS, and the Vaccine Confidence Project, we activated an emoji hashtag #vaccinated to show support for vaccination. This builds upon our earlier efforts to encourage people to #StayHome, #WashHands, and #WearAMask.

As health authorities deepen their understanding of COVID-19 and vaccination programs around the world, we will continue to amplify the most current, up to date, and authoritative information. We are all in this together, and we will continue to update you on our progress as we strive to play our part to protect the public conversation at this critical time.

This Tweet is unavailable



This Tweet is unavailable.

DEFENDANTS' EXHIBIT 176:

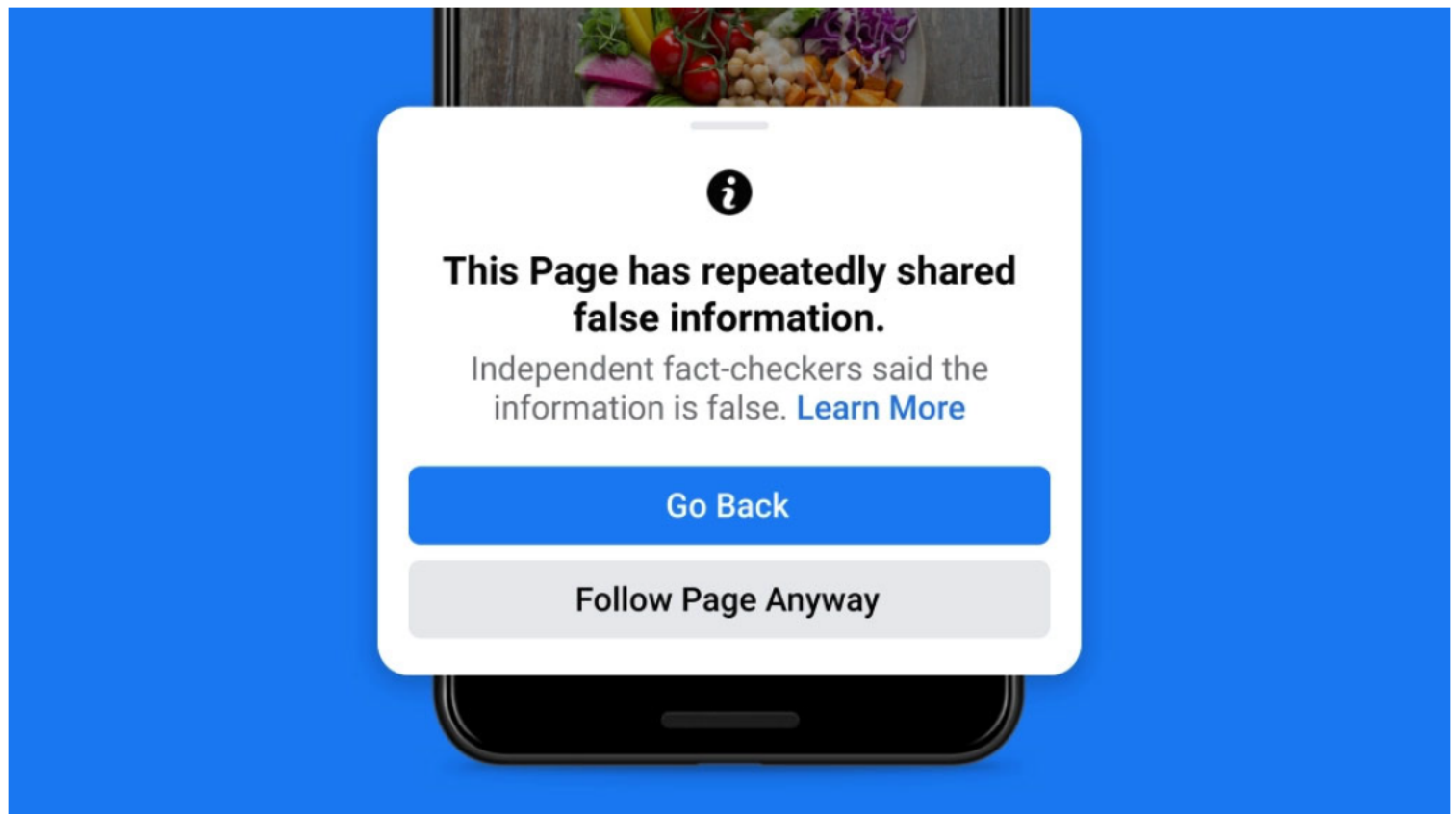


[Back to Newsroom](#)

Facebook

Taking Action Against People Who Repeatedly Share Misinformation

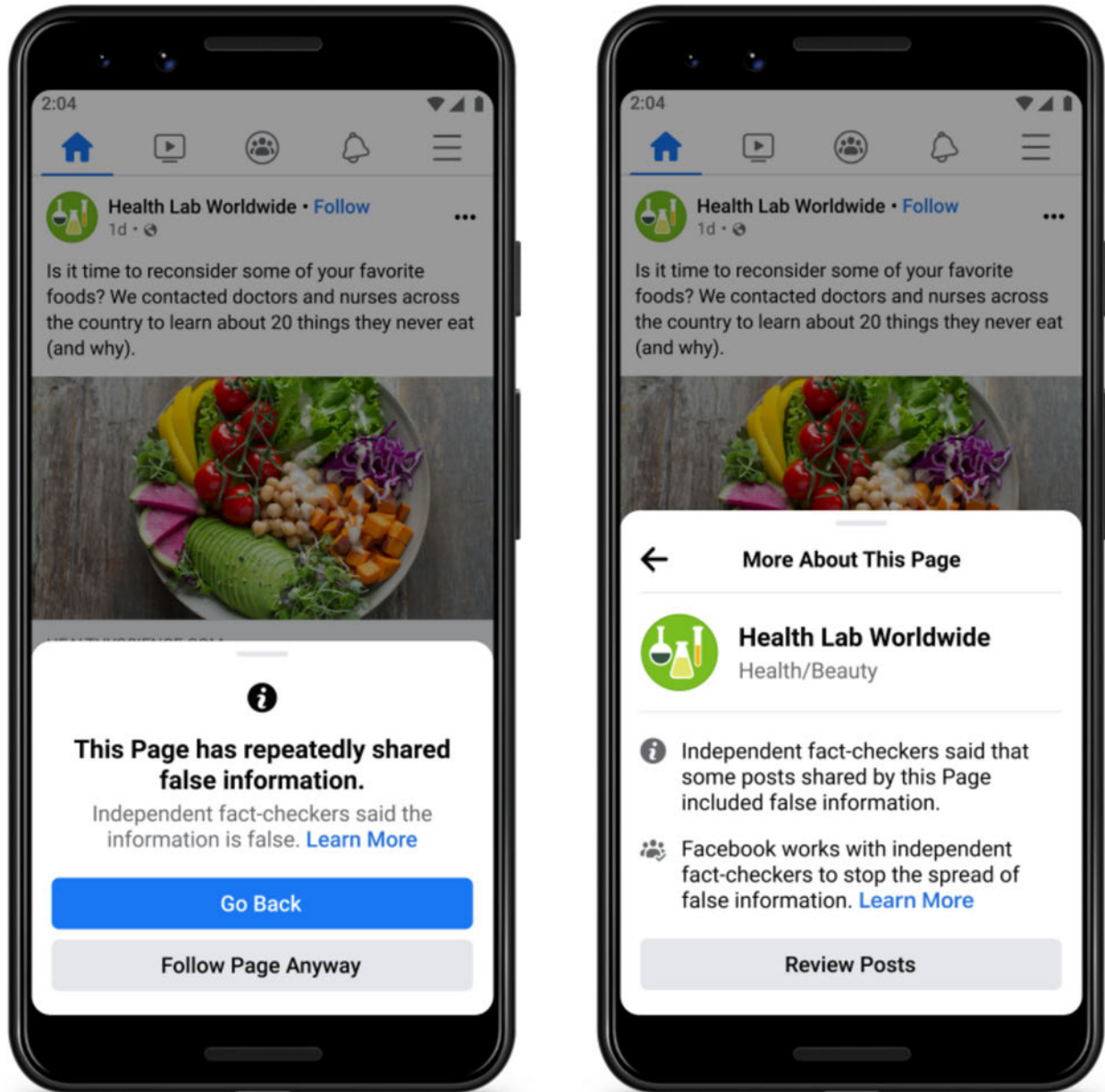
May 26, 2021



Today, we're launching new ways to inform people if they're interacting with content that's been rated by a fact-checker as well as taking stronger action against people who repeatedly share misinformation on Facebook. Whether it's false or misleading content about COVID-19 and vaccines, climate change, elections or other topics, we're making sure fewer people see misinformation on our apps.

More Context For Pages That Repeatedly Share False Claims

We want to give people more information before they like a Page that has repeatedly shared content that fact-checkers have rated, so you'll see a pop up if you go to like one of these Pages. You can also click to learn more, including that fact-checkers said some posts shared by this Page include false information and a link to more information about our fact-checking program. This will help people make an informed decision about whether they want to follow the Page.

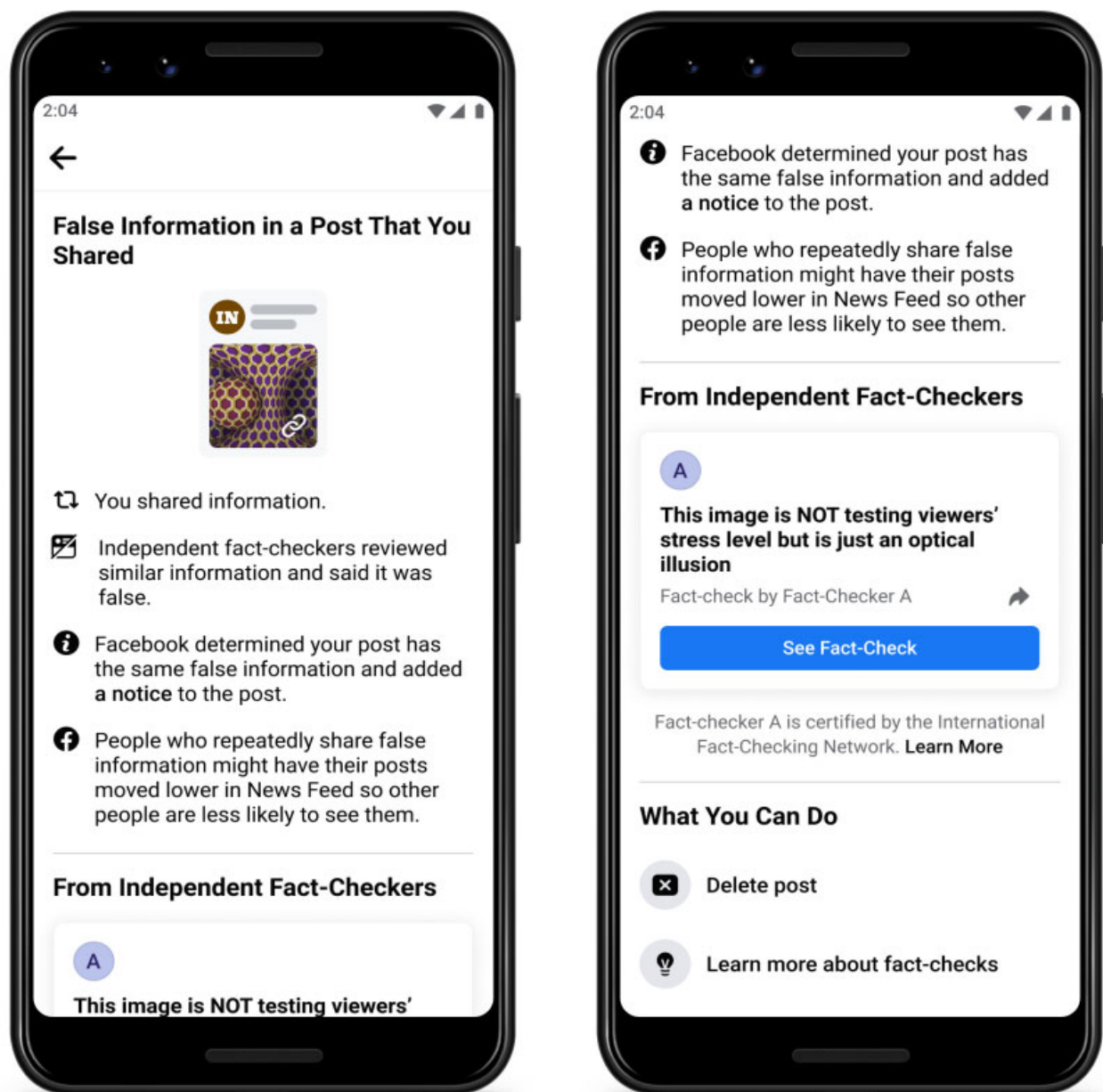


Expanding Penalties For Individual Facebook Accounts

Since launching our fact-checking program in late 2016, our focus has been on reducing viral misinformation. We've taken stronger action against Pages, Groups, Instagram accounts and domains sharing misinformation and now, we're expanding some of these efforts to include penalties for individual Facebook accounts too. Starting today, we will reduce the distribution of all posts in News Feed from an individual's Facebook account if they repeatedly share content that has been rated by one of our fact-checking partners. We already reduce a single post's reach in News Feed if it has been debunked.

Redesigned Notifications When People Share Fact-Checked Content

We currently notify people when they share content that a fact-checker later rates, and now we've redesigned these notifications to make it easier to understand when this happens. The notification includes the fact-checker's article debunking the claim as well as a prompt to share the article with their followers. It also includes a notice that people who repeatedly share false information may have their posts moved lower in News Feed so other people are less likely to see them.



Categories:
Facebook, Integrity and Security, Safety and Expression



Tags: Combating Misinformation

RELATED NEWS

Facebook

New Tools to Help Group Admins Protect, Manage and Grow Their Facebook Groups

We've added more features for Facebook group admins to help reduce their workload and grow their audiences.

March 9, 2022

Related Pages

Facebook

Topics

Company News

Technology and Innovation

Data and Privacy

Safety and Expression

Combating Misinformation

Economic Opportunity

Election Integrity

Strengthening Communities

Diversity and Inclusion

Featured News

Instagram

New Features on Instagram Reels: Trends, Editing and Gifts

April 14, 2023

Meta Quest

Peacock on Meta Quest: Stream Current Movies, Hit TV Shows and Live Sports in VR

April 12, 2023



Follow Us



Virtual reality



Smart glasses



About us



Our community



Our actions



Support



Community Standards

| Data Policy

Terms

| Cookie policy

United States (English) ▼